

Information Security Policy	
Version & release date:	V1.00 30/06/2025
Classification:	RESTRICTED
Distribution:	Pretense Flip N.V.
Status:	Policy in Progress

CONTENTS

1	Document Contents Definitions & Roles	1:9
1.1	Purpose	1:9
1.2	Scope	1:9
1.3	Definitions	1:10
2	Roles and Responsibilities	2:11
2.1	All Pretense Flip N.V. Employees	2:11
2.1.1	Implementation	2:12
2.1.2	Compliance	2:12
2.1.3	Physical Security	2:12
2.1.4	Security Awareness and Tamper Detection Training	2:12
2.1.5	Protection of Sensitive Information	2:12
2.1.6	Surveillance and Monitoring of Critical Infrastructure	2:12
2.1.7	Facility Access Controls	2:13
2.1.8	Systems Access	2:13
2.2	Senior Managers	2:13
2.3	IT Security Manager or Data Protection Officer (DPO)	2:13
2.3.1	Policy Oversight and Advisory Role	2:13
2.3.2	Collaboration and Enforcement	2:13
2.3.3	Incident Response – Personal Data Breaches ¹⁰	2:14
2.3.4	Policy Governance and Risk Management ¹¹	2:14
2.3.5	Third-Party Security Assurance ¹²	2:14
2.3.6	Policy Communication and Awareness ¹³	2:14
2.3.7	Board Engagement and Reporting	2:15
2.3.8	Industry Engagement and Best Practice Alignment	2:15
2.4	ICT Unit & Support:	2:15
2.5	The Management Team	2:15
2.6	The IT Administrator ¹⁴	2:15
2.6.1	System Use Consent and Monitoring ¹⁵	2:16
2.6.2	Password Management and User Identity Verification ¹⁶	2:16
2.6.3	Contractor and Vendor Access Control	2:17
2.6.4	Termination and Access Removal	2:17
2.6.5	Logging and Audit Trails	2:17

2.6.6	Authentication and Access Control Enforcement	2:17
2.6.7	Network and Physical Security Controls	2:17
2.6.8	Incident Response and Risk Management Participation	2:17
2.6.9	Security Awareness and Training Support	2:17
2.7	Internal Auditor / QA ¹⁷	2:18
2.7.1	Audit Participation and Planning	2:18
2.7.2	Compliance Assessment	2:18
2.7.3	Audit Criteria Development	2:18
3	Network & Internet Usage Policy ¹⁸	3:19
3.1.1	Purpose	3:19
3.1.2	Ownership	3:19
3.2	Usage Policy	3:19
3.2.1	Non-Business Browsing	3:19
3.3	Violations & Compliance	3:19
4	Acceptable Use Policy ¹⁹	4:20
4.1.1	Purpose	4:20
4.1.2	Scope	4:20
4.2	Technology Use and Data Ownership	4:21
4.3	Confidentiality, Security, and Proprietary Rights	4:22
4.4	Desk and Screen Security Standards ²¹	4:23
4.4.1	Clean Desk Requirements:	4:23
4.4.2	Clean Screen Requirements:	4:23
4.4.3	General Compliance:	4:23
4.4.4	Prohibited Use of Technology	4:23
5	Information Transfer Policy	5:27
5.1	Purpose	5:27
5.2	Policy	5:27
5.2.1	General Principles	5:27
5.3	Confidentiality and Non-Disclosure Agreements (NDAs)	5:27
5.4	Compliance and Enforcement	5:28
6	User Management Policy	6:29
6.1	Purpose	6:29
6.2	Scope	6:29

6.3	Logical Access Control Policy ²⁸	6:29
6.4	User Access Authorization	6:29
6.5	Access Review and Management ³¹	6:29
6.6	Prohibited Practices ³²	6:30
6.7	VPN WIFI	6:30
6.7.1	Key Access Requirements ³⁴	6:30
6.7.2	Control of Entry to a System ³⁶	6:31
6.7.3	Terminating User Access	6:32
6.7.4	Miscellaneous Access Controls	6:32
6.8	Compliance	6:33
7	Communication Security Policy	7:34
7.1	Purpose of This Policy	7:34
7.2	Company Ownership of Data	7:34
7.3	Proper Email Usage	7:34
7.4	Non-Business Email Use	7:34
7.5	Network Security Management	7:35
7.6	Security of Network Services ³⁹	7:35
8	Corporate Media Handling Policy	8:36
8.1	Purpose	8:36
8.2	Scope	8:36
8.3	Definitions	8:36
8.4	Policy Statements	8:36
8.4.1	General Principles for Media Management ⁴⁰	8:36
8.4.2	Management of Removable Media ⁴²	8:37
8.4.3	Hardcopy Media Handling ⁴³	8:37
8.4.4	Electronic Media Handling ⁴⁴	8:38
8.4.5	Media and Equipment Destruction & Sanitization ⁴⁵	8:38
8.4.6	Physical Media Transfer ⁴⁷	8:39
8.4.7	Backup Management ⁵⁰	8:40
8.5	Roles and Responsibilities	8:40
8.6	Training and Awareness	8:41
8.7	Policy Enforcement	8:41
8.8	Review and Updates	8:41

9	Information Classification and Handling Policy	9:42
9.1	Purpose	9:42
9.2	Data Roles and Responsibilities ⁵¹	9:42
9.2.1	Data Owners	9:42
9.2.2	Data Custodians/Processors	9:42
9.2.3	Data Users	9:42
9.3	Data Classification Standards ⁵²	9:42
9.3.1	Objective	9:42
9.4	Labelling of Information ⁵³	9:43
9.5	Data Access ⁵⁴	9:43
9.6	Technical Measures to Protect Data	9:44
10	Data Retention Policy	10:45
10.1	Purpose	10:45
10.2	Scope	10:45
10.3	Principles of Data Retention ⁵⁵	10:45
10.4	Data Retention Schedule	10:45
10.5	PCI DSS Requirements for Data Retention & Disposal	10:46
10.6	Prohibited Data Retention ⁵⁵	10:46
10.7	Permitted Data Retention & Protection ⁵⁶	10:47
10.8	Data Sources & Retention Specifics (PCI DSS)	10:47
11	Cryptographic Policy ⁵⁹	11:48
11.1	Purpose	11:48
11.2	Scope	11:48
11.3	Guiding Principles	11:48
11.4	Cryptographic Requirements	11:49
11.4.1	Information Classification and Cryptography Linkage	11:49
11.4.2	Approved Cryptographic Algorithms and Protocols	11:49
11.4.3	Cryptographic Key Management ⁶⁰	11:50
11.4.4	PCI DSS Specific Cryptographic Requirements	11:51
11.5	Application of Cryptography	11:51
11.5.1	Data at Rest Encryption	11:51
11.5.2	Data in Transit Encryption	11:51
11.5.3	Digital Signatures and Hashes	11:52

11.6	Roles and Responsibilities	11:52
11.7	Policy Enforcement	11:52
11.8	Policy Review	11:52
12	Encryption Policy	12:53
12.1	Purpose	12:53
12.2	Key Management and Access	12:53
12.3	Split Knowledge and Dual Control	12:53
12.4	Key Generation	12:53
12.5	Key Distribution	12:53
12.6	Key Storage	12:53
12.7	Transmission Over Untrusted Networks	12:54
12.8	Email Transmission of Confidential Information	12:54
12.9	Encryption of Wireless Networks	12:54
12.10	Non-console and Remote Administrative Access	12:54
13	Data Management Policy ⁶⁴	13:55
13.1	Purpose	13:55
13.2	Objectives	13:55
13.3	Data Protection Officer (DPO)	13:56
13.4	Data Protection Principles	13:56
13.4.1	Conditions for Lawful Processing	13:57
13.4.2	Processing of Special Categories of Personal Data	13:57
13.4.3	Automated Individual Decision Making	13:57
13.4.4	Limited Purposes	13:57
13.4.5	Data Minimisation	13:58
13.5	Accuracy and Up-to-Date Data	13:58
13.5.2	Integrity and Confidentiality	13:59
13.6	Data Inventory	13:59
13.7	Privacy Policy (External) ⁶⁵	13:60
13.8	Employee Data Processing ⁶⁶	13:60
13.8.1	Employee Privacy Notice	13:60
13.8.2	Data Processing Register for Employees ⁶⁶	13:60
13.9	Data Retention Policy	13:60
13.10	Data Breach Notification Policy	13:60

13.11	Data Subject Consent Form ⁶⁷	13:61
13.12	Data Protection Impact Assessment (DPIA) Register ⁶⁸	13:61
13.13	Data Breach Response and Notification Procedure ⁶⁹	13:61
13.14	Third-Party Processors	13:61
14	Change Management Policy	14:62
14.1	Initiating a Change	14:62
14.2	Testing Requirements	14:62
14.3	Change Reporting	14:62
15	Incident Management Policy ⁷¹	15:63
15.1	Purpose	15:63
15.2	Scope	15:63
15.3	Policy Statements	15:63
15.3.1	Incident Identification and Reporting	15:63
15.3.2	Incident Assessment and Triage ⁷³	15:63
15.3.3	Incident Response and Resolution ⁷⁴	15:64
15.4	Communication ⁷⁵	15:64
15.4.1	Post-Incident Review	15:64
15.4.2	Training and Awareness	15:64
15.5	Responsibilities	15:64
15.6	Policy Review	15:65
16	Information Security Risk Management Policy	16:66
16.1	Introduction & Purpose	16:66
16.2	Our Objectives	16:66
16.3	Risk Governance ⁷⁶	16:66
16.4	The Security Risk Register ⁷⁷	16:67
16.5	Risk Appetite ⁷⁸	16:67
16.6	Policy Development & Updates	16:67
16.7	Risk Communication & Review	16:68
17	Internet, Email, and Digital Asset Usage Policy	17:69
17.1	Purpose and Scope	17:69
17.2	Ownership and Monitoring	17:69
17.3	Internet Usage Policy ⁷⁹	17:69
17.4	Exceptions for Security Personnel	17:69

17.5	Email Usage Policy ⁷⁹	17:70
17.6	Non-Business Browse	17:70
17.7	Compliance and Enforcement ⁷⁹⁻⁸⁰	17:70
18	Pretense Flip N.V. Password Security Policy ⁸¹	18:71
18.1	Purpose	18:71
18.1.1	Who This Policy Applies To	18:71
18.2	Your Password, Your Responsibility	18:71
18.3	Crafting a Strong Password ⁸²	18:71
18.4	Maintaining Password Security	18:72
18.5	Critical System Passwords	18:72
18.6	Credentials Register	18:72
18.7	Password Monitoring and Enforcement	18:73
19	Anti-Virus policy	19:74
19.1	Purpose	19:74
19.2	Scope	19:74
19.3	Policy Statements	19:74
19.4	Anti-Malware Solution Deployment ⁸³	19:74
19.5	Anti-Malware Updates and Patching	19:75
19.6	Regular Scans ⁸⁴	19:75
19.7	Malware Detection and Response ⁸⁵	19:75
19.8	Removable Media and External Devices	19:76
19.9	Email and Web Security	19:76
19.10	User Awareness and Training ⁸⁵	19:76
19.11	Review and Monitoring ⁸⁶	19:76
20	Secure Mobile Computing	20:77
20.1	Purpose and Scope	20:77
20.2	Responsibilities and Accountabilities	20:77
20.3	Policy Directives	20:77
20.3.1	Device Physical Security & Access Control ⁸⁷	20:77
20.3.2	Data Protection and Encryption ⁸⁹	20:77
20.3.3	Responsible Device Usage	20:78
20.3.4	Incident Reporting	20:78
21	Internet & Software Usage Policy	21:79

21.1	Purpose	21:79
21.2	Scope	21:79
21.3	Policy Directives	21:79
21.3.1	Internet Usage	21:79
21.3.2	Software Usage	21:79
21.4	Incident Reporting	21:80
22	Security Testing and Vulnerability Management Policy	22:81
22.1	Purpose and Scope	22:81
22.2	Secure System Design and Deployment ⁹⁸	22:81
22.3	Change Detection and Integrity Monitoring ⁹⁹	22:81
22.4	Vulnerability Identification and Assessment ¹⁰⁰	22:82
22.5	Security Patch Management ¹⁰¹	22:83
23	Secure Access & Critical Systems Policy	23:84
23.1	Purpose & Scope	23:84
23.2	Controlled Access & Approval ¹⁰²	23:84
23.3	Authentication Requirements ¹⁰²⁻¹⁰³	23:84
23.4	Device Inventory & Identification ¹⁰⁴	23:84
24	Physical Security and Access Control Policy	24:85
24.1	Purpose & Scope	24:85
24.2	Access Control for Visitors & Personnel ¹⁰⁵	24:85
24.2.1	Visitor Management:	24:85
24.2.2	Personnel Access Control:	24:85
24.3	Defined Security Boundaries & Restricted Areas ¹⁰⁵	24:85
24.4	Physical Equipment Protection & Environmental Controls ¹⁰⁶	24:85
25	Appendix 1	25:87
26	References	26:87

Version Control Table

Version	Modified By	Date	Comments
V0.15	Maurizio Banavage	15/04/2025	Initial document Creation First Sector
V0.16-0.60	Maurizio Banavage	08/05/2025	Corrections and amendments according to Policies
V0.61	Maurizio Banavage	15/05/2025	Added sections 2 and 3
V0.61-0.70	Maurizio Banavage	20/05/2025	Corrections and Alignments with new directives

V0.71-0.85	Maurizio Banavage	23/05/2025	Added references Bottom of Document & Split of Doc
V0.86	Maurizio Banavage	03/06/2025	Added Section 4
V0.87-93	Maurizio Banavage	05/06/2025	Amendments and corrections on section 4
V0.94-97	Maurizio Banavage	08/06/2025	Corrections of DSS and ISO
V0.98	Maurizio Banavage	16/06/2025	Added Section 5 - Section 7
V.098 rev 5	Maurizio Banavage	18/06/2025	Added Sections 8 till 11
V0.99	Maurizio Banavage	26/06/2025	Added Sections 12 till 18 and validating Information
V1.00	Maurizio Banavage	30/06/2025	Added sections 19 till 23, validation in progress

INFORMATION SECURITY POLICY

1 Document Contents Definitions & Roles

1.1 Purpose

This document defines the information security requirements established by Pretense Flip N.V. (hereafter referred to as “Pretense Flip N.V.” or “the Company”) for all employees. These requirements reflect the Company’s commitment to protecting the information it relies upon to achieve its strategic and operational objectives.

Information is a critical asset to Pretense Flip N.V.. Therefore, appropriate safeguards must be in place to prevent unauthorized access, modification, disclosure, or destruction of data and related information.

This policy applies to all individuals who access, manage, or handle the Company’s information assets, including employees, contractors, vendors, service providers, and third parties. Compliance with this policy is mandatory.

In addition, this document outlines the procedures to be followed in the event of an actual or suspected information security breach. The breach response process is designed to:

- a) Confirm whether a security incident has occurred.
- b) Establish controls for the collection, preservation, and handling of evidence.
- c) Conduct investigations and produce accurate, timely reports in accordance with regulatory requirements and industry best practices.
- d) Identify corrective actions and implement measures to prevent recurrence of similar incidents.

1.2 Scope

This policy applies to all information owned, processed, or handled by Pretense Flip N.V., regardless of the format or medium—whether stored on computer systems, transmitted across networks, or maintained in physical form.

It is mandatory for all individuals working with the Company—including employees, contractors, consultants, vendors, and third-party service providers—to adhere to this policy, irrespective of their role, location, or relationship with Pretense Flip N.V..

The policy also extends to all *system components* within the Company’s information environment. *System components* refer to any network infrastructure, server, application, or device that stores, processes, transmits, or facilitates access to Company information.

Pretense Flip N.V.’s information environment encompasses any part of the network that contains or interacts with Company data. Examples of systems within the scope of this policy include, but are not limited to:

1. **Information storage systems:** e.g., databases, or desktop computers used by accounting to generate reports
2. **Information processing systems:** e.g., application servers, web servers
3. **Network devices managing data flow:** e.g., firewalls, routers, internal and perimeter security devices
4. **Media creation devices:** e.g., printers, fax machines, cloud-based backup solutions
5. **Support systems:** e.g., systems used for monitoring, logging, or administration of the information environment

6. All such components must be secured and managed in accordance with this policy to ensure the integrity, confidentiality, and availability of Company information.¹
7. The Company's information environment is that part of the network that possesses company information. For example, the following types of systems would be in scope for compliance within any environment:
 - A. Systems storing company information.
 - B. Such as databases, PCs used by accounting for generating reports. Systems processing company information.
 - C. Such as web servers, application servers, etc.
 - D. Network devices transporting or directing company information traffic. Such as border router, firewall, intranet firewall, etc.
 - E. Devices that create media containing company information. Such as fax machine, printer, backup cloud.
 - F. Support systems.
 - G. Such as Active Directory, PCs performing support functions such as system administration, etc.

It is the Company's policy to ensure that:

- A. All information is protected against unauthorised access. Confidentiality of information is assured.
- B. The integrity of the information is maintained. Regulatory and legislative requirements are met.
- C. Applicable Payment Card Industry Data Security Standard (PCI-DSS) requirements are met.
- D. Business Continuity Plans are produced, tested, and maintained.
- E. Information security awareness amongst all staff is created and maintained.²
- F. All breaches of information security, actual or suspected, are reported to and investigated by the Company's designated employee/s responsible for security.
- G. Copyright of intellectual property is respected. Information is protected against malicious code.

1.3 Definitions

Data Controller: the natural or legal person, public authority, agency or body which, alone or jointly with others, determines the purposes and means of processing of personal data.

Data Subject: means any person whose personal data is being collected, held or processed, e.g. applicant, employee.

DPO: An official who monitors compliance with data protection regulations, and acts as the point of contact with the relevant Data Protection Authority.

CTO: (Chief Technology Officer) is a high-level executive responsible for overseeing an organization's technological vision, strategy, and research and development efforts.

IDPC: Information and Data Protection Commissioner.

Personal data breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, **personal data** transmitted, stored or otherwise processed.

Information Security Incident: Any event that could compromise the confidentiality, integrity, or availability of information, or violate security policies

¹ ISO 27001 A.12.1² PCI DSS 12.6

Incident Response Team (IRT): The designated group or individuals responsible for leading and coordinating the response to information security incidents.

Chief Information Security Officer (CISO): Responsible for developing, implementing, and maintaining this policy, ensuring its alignment with ISO 27001 and PCI DSS, and advising on cryptographic best practices.

2 Roles and Responsibilities

Pretense Flip N.V. implements a Role-Based Access Control (RBAC) framework to ensure that access to data resources is restricted to authorised personnel only. Access permissions are granted based on predefined roles, which are aligned with an individual's job classification and functional responsibilities.

Prior to being granted access to any data resources, all employees must be assigned an appropriate role. Each role defines a specific set of access rights and privilege levels, tailored to the operational needs of the position. Access is granted on a least-privilege basis, ensuring that users are provided only with the minimum level of access necessary to perform their assigned duties.

Privileged user accounts are subject to stricter controls and are granted elevated access strictly in accordance with job requirements.

The assignment of roles and corresponding privileges is the responsibility of the internal IT Team. All role assignments must be documented, and prior written approval must be obtained and retained for audit and compliance purposes.

The Company creates and maintains complete information security responsibilities for all personnel³

Information security responsibilities include, but are not limited to:

Establishing, documenting, and distributing security incident response and escalation procedures⁴

2.1 All Pretense Flip N.V. Employees

All Pretense Flip N.V. employees have a duty to acknowledge the critical importance of the Company's information assets and to accept personal responsibility for their protection. Employees are expected to prevent misuse or any activity that could compromise the integrity, confidentiality, or availability of information systems.

In this regard, each employee shall:

1. Be fully aware of the implications of their actions in relation to information security practices and conduct themselves in a manner that supports the Company's security objectives.
2. Adhere to the principle that "Security is a shared responsibility," thereby contributing to the achievement of Pretense Flip N.V.'s operational and business goals.
3. Remain informed of, and comply with, the provisions of the Company's information security policies.
4. Review and formally acknowledge, by signature, their understanding of the Security Awareness Training and the Acceptable Use Policy agreements.
5. Appropriately classify any unlabelled confidential or sensitive information received, and ensure its disclosure is limited to authorised individuals on a need-to-know basis.

³ PCI DSS 12.4
⁴ PCI DSS 12.5.3

6. Promptly report any actual or suspected security incidents or breaches to their respective Senior Managers, in accordance with the Company's incident reporting procedures.

2.1.1 Implementation

Non-compliance with this Policy will be subject to management review and action in conformance with the Company's disciplinary procedures.

2.1.2 Compliance

All information held or processed by the Company, that is not publicly available, should be kept internal and undisclosed. Consequently, any breach of secrecy is a definite breach of the Company's policy.

This Security Policy is to be maintained and updated annually and when the environment changes. ⁵

An acceptable usage policy must also be maintained. ⁶

A risk assessment process is to be performed annually and upon significant changes to the environment. This should identify critical assets, threats, and other vulnerabilities. ⁷

The use of electronic communications and computer equipment is regulated under relevant provisions of the national Criminal Code. The protection of personal data is governed by national data protection legislation. This policy is intended to guide the Company's employees in ensuring compliance with all relevant legal obligations.

2.1.3 Physical Security

It is company policy to disable unused network ports. No one is allowed to connect devices to the network unless explicitly authorised by the IT Administrator.

2.1.4 Security Awareness and Tamper Detection Training

All personnel must receive appropriate training to enable them to identify and respond to any attempted tampering with, or unauthorized replacement of, IT equipment and related devices. This training shall be conducted periodically and updated as necessary to address emerging threats and technologies.

2.1.5 Protection of Sensitive Information

Hard-copy documents and electronic media containing sensitive or confidential information must be safeguarded through the implementation of suitable physical access controls. These controls shall be designed to prevent unauthorized access, modification, or removal of such materials.

2.1.6 Surveillance and Monitoring of Critical Infrastructure

Closed-circuit television (CCTV) systems shall be installed and maintained in all server rooms, data centres, and other secured facilities housing systems that process or store sensitive, confidential, or cardholder data. Recorded footage must be retained for a minimum period of three (3) months, unless a different retention period is mandated by applicable laws or regulatory requirements.

⁵ PCI DSS 12.1, PCI-DSS 12.1.1

⁶ PCI DSS 12.3

⁷ PCI DSS 12.2

2.1.7 Facility Access Controls

Facilities containing systems that store, or process confidential or sensitive data must be secured using appropriate physical security measures. These measures shall include, but are not limited to, access control systems, visitor logging procedures, and physical barriers, and must be capable of both limiting and monitoring physical access to such systems.

2.1.8 Systems Access

Each computer system must implement either an automated or procedural access control mechanism. The requirements above are for authenticating all system users.

This process shall include the following requirements:

1. Generic user IDs and default passwords must be disabled or removed. Each user must be assigned a unique user ID.
2. All system and application accounts must be secured through password authentication. Passwords or passphrases must be a minimum of ten (10) characters in length.⁸
3. Passwords must be complex, containing a mix of alphabetic, numeric, and special characters. New passwords must not duplicate any of the last Twelve (12) previously used passwords.
4. User accounts will be locked after a maximum of ten (10) consecutive failed login attempts.
5. Locked accounts must remain inaccessible for at least thirty (30) minutes or until reactivated by the IT Administrator.⁹
6. Idle systems or sessions must automatically log out after fifteen (15) minutes of inactivity.
7. Passwords must be changed at least once every ninety (90) days.

2.2 Senior Managers

Senior Managers are responsible for assessing, managing, and escalating reported incidents. Their responsibilities include:

1. Gathering all relevant information by requesting additional details as necessary.
2. Managing the incident directly or escalating it to appropriate stakeholders when required.
3. Ensuring that all required incident documentation (refer to Section 6: Reporting) is completed and properly filed.
4. Notifying the Pretense Flip N.V. IT Security Manager in cases involving actual or suspected breaches of personal data.

2.3 IT Security Manager or Data Protection Officer (DPO)

2.3.1 Policy Oversight and Advisory Role

The IT Security Manager holds direct responsibility for maintaining Pretense Flip N.V.'s information security policies. This includes providing expert advice and guidance on security measures and supporting their effective implementation across the organization.

2.3.2 Collaboration and Enforcement

The IT Security Manager collaborates closely with Pretense Flip N.V. personnel and third-party entities involved in protecting the Company's information assets. The goal is to enforce established policies, identify areas of concern, and recommend or implement appropriate improvements.

⁸ PCI DSS 8.3.8

⁹ PCI DSS 8.3.9

^{8 & 9} ISO 27001:2022 A.5.17

2.3.3 Incident Response – Personal Data Breaches¹⁰

The IT Security Manager & Data Protection Officer (DPO) is engaged specifically in incidents involving actual or suspected breaches of personal data. Responsibilities include:

1. Ensuring all relevant details are captured using the Personal Data Breach Incident Report Form (see Appendix 1).
2. Acting as the designated liaison between Pretense Flip N.V. and the relevant Data Protection Authority, and ensuring the timely submission of required reports..
3. Coordinating communications with affected data subjects in accordance with applicable data protection laws. Maintaining comprehensive and up-to-date records of all personal data incidents and breaches.
4. Monitoring incident trends and overseeing implementation of corrective and preventive actions to reduce recurrence.

2.3.4 Policy Governance and Risk Management¹¹

1. Making strategic decisions regarding the content and enforcement of Pretense Flip N.V.'s information security policies.
2. Granting exceptions to these policies on a documented, case-by-case basis with appropriate justification and prior approval.
3. Leading a formal risk assessment at least annually to evaluate emerging threats and vulnerabilities and determine appropriate mitigation controls.
4. Reviewing all information security policies and procedures at least once annually, or more frequently if warranted by changes in business operations or the threat landscape.
5. Creating, maintaining, and communicating the Information Security Management System (ISMS) in line with regulatory and industry requirements.

2.3.5 Third-Party Security Assurance¹²

Ensuring that all third parties who process or access Pretense Flip N.V. information are contractually obligated to comply with PCI DSS and other relevant data protection requirements and accept accountability for the security of the Company's information they handle.

2.3.6 Policy Communication and Awareness¹³

Distributing information security policies, acceptable use guidelines, and other relevant documentation to all applicable users, including employees, contractors, service providers, and business partners.

Maintaining a record of all signed Security Awareness, Acceptable Use, and Authorisation Request Forms in employee personnel files.

¹⁰ PCI DSS 12.4

¹¹PCI DSS 12.5.3

¹²PCI DSS12.1

¹³ ISO 27001 A.6.1.4

2.3.7 Board Engagement and Reporting

Providing the Board of Directors with timely and relevant information to support their oversight responsibilities. This includes enabling informed decision-making on matters relating to risk, information security, and operational resilience.

2.3.8 Industry Engagement and Best Practice Alignment

Maintaining active contact with industry groups, forums, and special interest organizations to remain informed of evolving best practices, receive early alerts, and participate in knowledge sharing relevant to information security.

2.4 ICT Unit & Support:

The ICT Unit must and have the duty to:

1. Investigate information security incidents of a technical nature.
2. Handle escalated cases and assist with the investigation, containment, threat eradication and incident resolution measures.
3. Review technical controls and assist with the implementation of new security controls to prevent incidents from re-occurring.
4. Carry out evaluation of past incidents and follow up with the unit senior managers ensure that follow-up actions have been taken.

2.5 The Management Team

The Management Team is responsible for implementing this policy within their business area and ensuring that all employees understand their obligation to protect Pretense Flip N.V.'s assets and comply with security standards and related procedures.

1. All employees have a responsibility to conduct themselves in an ethical manner: Data and information obtained inappropriately should not be used.
Finding a system weakness is not a license to take advantage of it.
2. Every user has a responsibility to carry out their work diligently and will be held accountable for misuse of the Company's computer systems.
3. When the confidentiality of information is unclear, its classification should be ascertained.
4. Any known violation or system weakness should be reported to the person/s responsible for the Company's security or to the respective line manager.
5. All intrusions should be reported and investigated, and the Incident Response Policy should be adhered to.

2.6 The IT Administrator ¹⁴

The **IT Administrator** serves as the operational liaison between Pretense Flip N.V.'s information security policies and the implementation of technical controls across the Company's networks, systems, and data environments.

¹⁴ISO/IEC 27001:2022
Annex A.9.2, A.9.4, A.12.2.1, A.13.2.3

2.6.1 System Use Consent and Monitoring ¹⁵

All users of Pretense Flip N.V. systems explicitly consent to monitoring as a condition of access. Users are advised that:

"Anyone using this system expressly consents to such monitoring and acknowledges that, should such monitoring reveal evidence of criminal or unauthorized activity, such evidence may be shared with law enforcement or other relevant authorities in accordance with legal and regulatory obligations."

This banner must be displayed on all systems capable of showing a login notice.

2.6.2 Password Management and User Identity Verification¹⁶

Initial system passwords must be unique, randomly generated, and compliant with the Company's Password Policy.

Account creation requests must specify access either explicitly or via a "role" that has been drawn to the required access. New accounts created by mirroring existing user accounts must be audited against the explicit request or roles for appropriate access rights. If a user requests a password reset via phone, email, web, or another non-face-to-face method, that user's identity must be verified before the password is reset.

Access should be removed immediately upon notification that access is no longer required. Written procedures must be in place to ensure that access privileges of terminated or transferred users are revoked as soon as possible.

Whenever possible, users who are on leave-of-absence or extended disability should be suspended from the system. User IDs shall be disabled after sixty (60) days of inactivity. After an additional thirty (30) days, disabled user IDs must be eradicated. These requirements may not apply to certain specialised accounts (such as NT Admin, root, etc.) In those instances, the IT Administrator must provide a written waiver to the Information Security Team and document the compensating controls around access to the accounts. All computer resources capable of displaying a custom sign-on or similar message must display the following message as part of the login process:

- A. Users must be required to change system-assigned passwords upon first login.
- B. Prior to resetting a user's password, the IT Administrator must verify the user's identity using formal verification procedures. Each business unit is responsible for establishing local identity validation procedures to support this requirement.

¹⁵⁻¹⁶ISO/IEC 27001:2022
Annex A.6.3, A.5.18, A.5.10
¹⁶PCI DSS 8.22, 8.24, 12.6

2.6.3 Contractor and Vendor Access Control

1. **Contractor accounts** must be pre-approved by the Internal IT Team and configured with automatic expiration aligned to the contract end date. Extensions must be requested and approved in writing.
2. **Vendor accounts** used for remote maintenance must be enabled only during the approved maintenance window and disabled immediately after the task is completed.

3. Contractor and vendor accounts must be actively monitored throughout their period of use. The IT Administrator is responsible for logging, reviewing, and maintaining appropriate access control for these accounts.

2.6.4 Termination and Access Removal

User access must be revoked immediately upon notification of termination or when access is no longer required. Timely deprovisioning of access is mandatory to reduce the risk of unauthorized system use.

2.6.5 Logging and Audit Trails

1. The IT Administrator must enable and maintain **audit logs** that capture both user and administrative activities across all critical systems.
2. Logs must be retained for a **minimum of one (1) year**, with **at least 90 days of logs available for immediate online access**.
3. Logs must be protected against tampering and unauthorized access and reviewed regularly for suspicious activity.

2.6.6 Authentication and Access Control Enforcement

1. Authentication must be enforced on all systems, particularly those interfacing with sensitive or regulated data (e.g., database systems).
2. The IT Administrator is responsible for configuring, validating, and maintaining secure authentication mechanisms, including multi-factor authentication where required.

2.6.7 Network and Physical Security Controls

1. Maintain an up-to-date network topology diagram that includes all infrastructure, including wireless networks.
2. Physical access to network jacks, wireless access points, and other critical infrastructure (e.g., gateways, routers, handheld devices) must be restricted to authorized personnel only.

2.6.8 Incident Response and Risk Management Participation

1. Participate in the Company's formal **risk assessment process** to help identify, evaluate, and mitigate information security risks.
2. Respond to detected or reported **security threats and incidents** in accordance with the Company's Incident Response Policy and procedures.
3. Maintain and support the availability, integrity, and confidentiality of the IT & Communications (IT&C) infrastructure.

2.6.9 Security Awareness and Training Support

- Assist in raising user awareness on IT security risks and promoting secure practices across all departments.
- Support training efforts led by the Information Security Team by identifying security issues that may affect end users or business operations.

2.7 Internal Auditor / QA ¹⁷

The Internal Auditor / Quality Assurance (QA) function is responsible for conducting internal audits to evaluate the effectiveness and conformity of the Information Security Management System (ISMS). An audit is defined as a systematic, independent, and evidence-based process for obtaining objective evidence and making impartial assessments to determine the extent to which audit criteria are fulfilled.

Specific Responsibilities Include:

2.7.1 Audit Participation and Planning

Participate in and support the planning, execution, and continual improvement of the audit management process in accordance with the internal audit schedule.

Audit Reports

Prepare, document, and formally distribute Internal Audit Reports, including audit findings, observations, and nonconformities, in a timely manner to relevant stakeholders.

2.7.2 Compliance Assessment

Assess the organization's compliance with the information security controls and risk treatments documented in the Statement of Applicability (SoA) and evaluate whether controls are being effectively implemented and maintained.

2.7.3 Audit Criteria Development

Develop and refine audit criteria to ensure they are comprehensive, relevant, and aligned with regulatory requirements, and internal policies, thereby increasing audit accuracy and reliability.

3 Network & Internet Usage Policy¹⁸

This Section outlines Pretense Flip N.V.'s policy on employee responsibilities for Internet usage over the Company's network.

3.1.1 Purpose

Employee access to the Internet is provided solely to support the performance of job-related duties and to facilitate the daily operations of the Company.

3.1.2 Ownership

All computers, network components, and installed software are the property of the Company. Any data stored on Company-owned computers, devices, storage media, or within the Company network is also considered Company property. The Company reserves the right to monitor and inspect its systems, including computers, network devices, and audit logs, to ensure appropriate and authorized use of Internet access. Usage of computer systems for purposes not related to Internet access is governed by separate policies.

3.2 Usage Policy

All employees requiring Internet access must use Company-approved software and connect through authorized Internet gateways. Accessing illicit, unauthorized, or potentially harmful websites—including hacker-related or otherwise suspicious sites—is strictly prohibited.

Downloading software, executable files, or other potentially unsafe content from the Internet is not allowed without prior approval.

Employees are reminded that web activity is logged, and all browsing activity can be traced.

IT personnel who require access to high-risk or questionable sites for legitimate security research or system vulnerability assessments must obtain prior written authorization. Such activities must be conducted on isolated systems that do not contain sensitive or business-critical data, and all precautions must be taken to avoid introducing risk to the Company network.

3.2.1 Non-Business Browsing

Limited personal browsing may be permitted during designated break times or free periods, such as for personal research or non-business use. However, all usage must remain in compliance with the Company's Internet and acceptable use policies.

3.3 Violations & Compliance

Any violation of this policy may result in disciplinary action, up to and including termination of employment and, where applicable, legal proceedings. Employees who become aware of any breach of this policy are required to report it promptly to the designated Information Security Officer. All reports will be treated confidentially, and the identity of the reporting individual will be protected to the fullest extent possible.

¹⁸ ISO 27001 2022 Annex A controls
A.6.2.1, A.9.1.2, A.9.2.3, A.13.2.1, and A.18.1.

4 Acceptable Use Policy¹⁹

4.1.1 Purpose

The purpose of this Acceptable Use Policy is to establish clear and lawful guidelines for the proper use of the Company's information systems, technology assets, and digital services. This policy aims to protect the integrity, confidentiality, and availability of Company resources while supporting a professional environment rooted in openness, trust, and integrity.

The Company affirms that this policy is not intended to impose unreasonable restrictions that conflict with its organizational culture. Rather, it is designed to promote responsible and secure use of technology in a way that aligns with the Company's business objectives and legal obligations.

Management is fully committed to safeguarding the interests of the Company, its employees, clients, account holders, and business partners by mitigating the risks associated with inappropriate, illegal, or damaging use of information technology systems—whether such use is intentional or unintentional.

This policy applies to all users of Company-provided or Company-authorized IT resources, including but not limited to:

1. Computer hardware and peripherals
2. Software and operating systems
3. Electronic communication tools (e.g., email, messaging, collaboration platforms)
4. Internet and intranet access, including web browsing and file transfer protocols (FTP)
5. Network accounts and cloud-based services
6. Digital documentation, media, and storage systems

All such systems are the property of the Company and are to be used primarily for legitimate business purposes that support the Company's operations and the interests of its customers.

Compliance with this policy is essential. Improper use of Company IT resources may lead to security threats such as malware infections, data breaches, reputational harm, and legal exposure. Therefore, adherence to this policy is mandatory and non-compliance may result in disciplinary action, up to and including termination of employment and/or legal proceedings, as appropriate.

4.1.2 Scope

This policy applies to all personnel engaged by Pretense Flip N.V., including full-time and part-time employees, contractors, subcontractors, consultants, temporary staff, and any individuals affiliated with third-party service providers. It covers the use of all Company-owned or Company-leased equipment, systems, networks, and digital assets, including but not limited to hardware, software, communication tools, and cloud-based platforms.

¹⁹ISO 27001:2022
A.6.2.1, A.9.2.3

The policy also extends to any services operating on these systems and any associated documentation related to Company products, services, clients, partnerships, or internal operations.

Technologies in scope include but are not limited to ²⁰

1. Remote access
2. Wireless networks
3. Laptops
4. Tablets
5. Smartphones
6. Removable electronic media
7. Email
8. Internet

4.2 Technology Use and Data Ownership

While the Company's Internal IT Team aims to support a reasonable level of privacy for users, all data created, stored, transmitted, or processed using Company systems is the sole property of the Company. Employees should have no expectation of personal ownership over any data or content residing on Company-owned or managed devices and platforms.

Access to Company technology, including devices, systems, and electronic media, must be explicitly authorized by designated personnel. Unauthorized use of such resources is strictly prohibited.

Employees are expected to exercise sound judgment regarding the personal use of Company resources. Limited personal use may be permitted, provided it does not interfere with job responsibilities or violate any applicable Company policies, including the [Internet and Email Usage Policy](#). In cases of uncertainty, employees must consult their direct supervisor for guidance.

Use of Company laptops or devices for personal purposes is strongly discouraged, especially when it may involve mixing Company-sensitive data with personal information. Users must not apply personal passwords on Company systems or use Company account credentials on personal devices.

To protect sensitive or confidential information, it is strongly recommended that such data be encrypted or, at a minimum, protected by robust password controls, in line with the Company's Information Security Policy.

For operational security and network maintenance purposes, authorized personnel may monitor systems, equipment, and network traffic at any time, without prior notice. The Company reserves the right to conduct audits of its networks, systems, and data to ensure compliance with this policy and all applicable security standards.

²⁰PCI DSS 12.3

All documentation, reports, or other work products created, stored, or processed on Company systems are considered Company property and must be handled in accordance with applicable data classification, retention, and handling policies.

4.3 Confidentiality, Security, and Proprietary Rights

All information stored, transmitted, or processed via the Company's Internet, Intranet, and Extranet systems must be classified in accordance with the guidelines established by management. Confidential information includes, but is not limited to, corporate strategies, competitive intelligence, trade secrets, product specifications, customer data, credit card information, and proprietary research. Employees must take all appropriate measures to safeguard this information against unauthorized access.

Passwords must be kept confidential and must not be shared. Users are individually accountable for maintaining the security of their passwords and associated accounts.

All desktop computers, laptops, and workstations must be secured using password-protected screensavers with automatic activation set to 15 minutes or less. Alternatively, users must log off or lock their sessions when leaving their workstations unattended.

Where passwords alone are insufficient to protect sensitive data, encryption must be used. Only secure, approved encryption algorithms and key management practices are permitted.

Given the heightened risk associated with portable devices, only business-critical data should be stored on them and only for the time necessary. Confidential data on such devices must be encrypted using approved standards.

When posting to public forums or newsgroups using Company email addresses, employees must include disclaimers stating that the views expressed are their own and do not reflect those of the Company—unless such communication is part of their official responsibilities.

Any device—whether personally or Company-owned—connected to the Company's networks must run approved, continuously operating antivirus software with up-to-date virus definitions, unless otherwise specified by departmental policies.

Employees must exercise extreme caution when handling email attachments from unknown sources, as they may contain malware such as viruses, ransomware, or Trojan horses. Sensitive documents and information must be cleared from desks and locked securely when unattended or at the end of the workday.

File cabinets containing sensitive materials must be kept locked when not in use. Keys should not be left unsecured. Laptops must be secured using locking cables or locked in drawers when not in active use.

Passwords and other sensitive data must not be written on sticky notes or any other unencrypted device, nor transmitted via unencrypted email or unsecured messaging platforms.

4.4 Desk and Screen Security Standards²¹

To maintain a secure and professional work environment and protect sensitive information, the following Clean Desk and Clean Screen practices must be observed by all employees, contractors, and affiliates—without exception.

4.4.1 Clean Desk Requirements:

1. Reports, documents, or materials containing sensitive or confidential information must not be left unattended on desks or in any accessible area where unauthorized individuals may view or access them.
2. At the end of each working day, all papers, notes, and portable storage devices must be cleared from the desk and properly secured.
3. Such information must be securely stored in locked drawers, cabinets, or other authorized storage when not actively in use or when the employee is away from their desk.

4.4.2 Clean Screen Requirements:

1. Computer screens must be locked or logged off when unattended to prevent unauthorized access or viewing.
2. Employees must avoid placing **post it notes**, printed passwords, or stickers on monitors or workstations that could disclose sensitive information or clutter the workspace.

4.4.3 General Compliance:

1. This policy applies uniformly to all personnel, including full-time employees, part-time staff, contractors, and temporary affiliates.
2. Adherence to this policy is essential for supporting confidentiality, reducing information leakage risks, and maintaining ISO 27001 compliance.

Failure to comply with this policy may result in disciplinary action in accordance with the Company's information security and HR procedures.

4.4.4 Prohibited Use of Technology

The activities outlined in this policy are generally not permitted. However, exemptions may be granted where specific job functions necessitate such actions (e.g., members of the Internal IT Team may disable network access to a device if it is negatively impacting production systems).

Under no circumstances may employees use Company-owned resources to engage in activities that are unlawful under local, national, or international law.

While not exhaustive, the examples below provide a framework for understanding what constitutes unacceptable use of Company technology resources.

²¹ISO 27001 A.11.2.9

4.4.4.1 Prohibited System and Network Activities²²

The following actions are strictly forbidden and are not permitted under any circumstances:

1. **Intellectual Property Violations:** This includes unauthorized installation, distribution, or use of software or content protected by copyright, trade secret, patent, or other intellectual property laws. Examples include using pirated software or copying copyrighted materials (e.g., digital images, music, software) without proper authorization or licensing.
2. **Export Control Violations:** Transmitting or exporting software, technical data, encryption tools, or technologies in violation of applicable export control laws is prohibited. Employees must consult management before exporting any such materials.
3. **Malicious Software:** Introducing any form of malicious code, such as viruses, worms, trojans, malware, ransomware, or email bombs, into the Company's systems is strictly forbidden.
4. **Credential Misuse:** Sharing passwords or account access with unauthorized individuals—including family members when working remotely—is not allowed.
5. **Data Transfer Restrictions:** Moving sensitive or confidential Company data between Company and personal or home systems without explicit management approval is prohibited.
6. **Harassment or Offensive Content:** Using Company systems to create, transmit, or store content that violates sexual harassment laws or contributes to a hostile work environment is strictly forbidden.
7. **Fraud and Misrepresentation:** Offering fraudulent products, services, or representations through Company accounts is prohibited. Making unauthorized warranty claims or other assurances is not allowed unless it falls within the employee's job scope.
8. **Security Breaches and Network Disruption:** Unauthorized access to data, systems, or accounts not assigned to the employee, as well as activities such as denial-of-service attacks, packet spoofing, forged routing, or network sniffing for malicious purposes, are violations of this policy.
9. **Unauthorized Scanning and Monitoring:** Performing port scans, security scans, or intercepting data not intended for the employee's system is not allowed unless specifically authorized by management.
10. **Bypassing Security Controls:** Attempting to disable, bypass, or otherwise interfere with authentication or security mechanisms is prohibited.
11. **Session Interference:** Using scripts, programs, or messages to disrupt or disable another user's session, whether locally or over a network, is not permitted.
12. **Disclosure of Internal Information:** Sharing internal information, such as employee directories or customer lists, with external parties without authorization is prohibited.

This policy aims to protect the integrity, confidentiality, and availability of the Company's technology systems and data. All employees are expected to understand and adhere to these guidelines. Violations may result in disciplinary action, up to and including termination, and potential legal consequences.

4.4.4.2 Acceptable Use of Critical Technologies

4.4.4.2.1 The use of critical technologies must strictly adhere to the following requirements to ensure the protection of all data, such as cardholder data and other personal information, to maintain compliance with relevant data security and privacy regulations.

4.4.4.2.2 USAGE AUTHORIZATION²³

1. The use of any critical technology must be explicitly approved by designated and authorized personnel prior to deployment or access.
2. Usage must align with business needs and be documented, reviewed, and authorized in accordance with formal change control or access management processes.

4.4.4.2.3 AUTHENTICATION REQUIREMENTS²⁴

All access to critical technologies must be secured with strong authentication mechanisms, including unique user IDs, complex passwords, multi-factor authentication, or equivalent controls that meet PCI DSS standards.

4.4.4.2.4 DEVICE AND USER INVENTORY²⁵

1. A comprehensive and continuously maintained inventory must be kept, identifying all devices and personnel authorized to use critical technologies
2. Each device or user must be uniquely identifiable within the inventory.

4.4.4.2.5 OWNERSHIP AND ACCOUNTABILITY²⁵

1. Every asset and technology in use must have a clearly designated owner responsible for its security, purpose, and compliance.
2. Contact information and the functional purpose for each critical technology must be documented and readily accessible.

4.4.4.3 Network Access Controls

All critical technologies must be used only from approved network zones or segments. Usage from unapproved or untrusted networks is strictly prohibited unless explicitly authorized and monitored.

4.4.4.3.1 SESSION MANAGEMENT

Remote access technologies must include automatic session timeouts or disconnection after a pre-defined period of inactivity, as specified by security policy.

²³PCI DSS 12.3.1

²⁴PCI DSS 12.3.3

²⁵ISO27001:2022
A.5.9

4.4.4.3.2 THIRD-PARTY REMOTE ACCESS

1. Remote access for vendors, contractors, or business partners must be enabled only when required for specific tasks and must be immediately disabled once the task is complete.
2. Such access must be tightly controlled, monitored, and logged in accordance with security procedures.

4.4.4.3.3 CARDHOLDER DATA RESTRICTIONS

1. Under no circumstances may cardholder data be copied, transferred, or stored on local hard drives or removable media during or after remote access sessions.
2. Access to cardholder data via remote technologies must be restricted to viewing only, unless otherwise approved and secured according to PCI DSS guidelines.

4.4.4.4 Compliance and Enforcement

Violations of this policy will result in disciplinary action, up to and including termination of employment, and may lead to legal consequences. All activity is subject to logging, monitoring, and audit.

4.4.4.5 Asset Management and Responsibility

4.4.4.5.1 ASSET INVENTORY²⁵

The Company must maintain a detailed inventory of all assets associated with information systems and processing environments, including hardware, software, and data.

4.4.4.5.2 OWNERSHIP ASSIGNMENT

Ownership must be assigned to each asset to ensure accountability for maintenance, protection, and compliance.

4.4.4.5.3 ACCEPTABLE USE

Clear, documented rules for the acceptable use of information assets must be communicated to all employees and third parties with access.

4.4.4.5.4 RETURN OF ASSETS

A formal process must be in place to ensure the return of all assets (e.g., laptops, tokens, credentials) upon termination of employment or end of engagement with third parties.

5 Information Transfer Policy

5.1 Purpose

An "Information Transfer Policy" (also sometimes referred to as an "Information Transparency Policy" in a broader sense) is a crucial set of guidelines and procedures that dictate how information is shared both within and outside an organization.

5.2 Policy

5.2.1 General Principles

Formal agreements must be in place between the Company and any third party involved in *information transfer* to ensure the secure exchange of business data. This includes outlining responsibilities and security measures for all shared information.

5.2.1.1 Secure Transfer Methods

1. Avoid standard messaging and email for sharing sensitive information, such as confidential documents or Permanent Account Numbers (PANs). These platforms lack the necessary security for such data.²⁶
2. Always use secure document management systems when transferring sensitive documents. These systems should offer features like *collaboration tools* and *role-based sharing* to control access effectively.²⁷
3. Employ cryptographic techniques (like encryption) to safeguard the *confidentiality, integrity, and authenticity* of all sensitive information during transfer. This protects data from unauthorized access or alteration.

5.2.1.2 Data Retention and Approved Platforms

All business correspondence, regardless of its sensitivity, must adhere to established *retention and disposal guidelines* and comply with relevant *local legislation*.

The Company will *specify and approve designated platforms* for electronic messaging, both internally and with third parties. Any other messaging platforms are *strictly prohibited* for official use.

5.3 Confidentiality and Non-Disclosure Agreements (NDAs)

We take the protection of our sensitive information seriously. Therefore, requirements for confidentiality and non-disclosure agreements are mandatory. These requirements will be regularly reviewed and meticulously documented to ensure they remain current and effective.

To streamline this process, a standard Non-Disclosure Agreement (NDA) template will be maintained. This template will be the foundation for all NDAs and must be adapted as needed to fit the specific circumstances of each agreement. It's critical that no sensitive company information is exchanged with any third party until a mutually agreed-upon NDA is fully executed.

²⁶ PCI DSS 4.2

²⁷ ISO 27001 A.13.2.2-3

Our NDA template will comprehensively cover:

1. A clear and precise definition of the information subject to protection. This ensures all parties understand what's confidential.
2. The agreed-upon duration of the confidentiality obligations.
3. Specific actions required upon the termination of the agreement, including the return or destruction of confidential information.
4. The precise responsibilities and actions signatories must undertake to prevent unauthorized disclosure. This outlines their proactive role in safeguarding information.
5. Clear delineation of ownership for all information, trade secrets, and intellectual property.
6. The stipulated actions to be taken in the event of a breach of the agreement. This provides a clear roadmap for addressing violations.
7. Crucially, all Non-Disclosure Agreements must fully comply with all applicable laws and regulations.

5.4 Compliance and Enforcement

1. Adherence to this Information Transfer Policy is mandatory for all employees and third parties. Any violation will result in swift disciplinary action, up to and including termination of employment and/or legal action, as deemed appropriate.
2. We encourage a culture of vigilance. Employees are required to report any misuse of the Company's electronic systems (including email) or any observed violations of this policy to their manager or the designated official. We assure you that the identity of any reporting staff member will be treated with the strictest confidence to protect them.
3. Finally, remember that computer misuse is a serious offense that can constitute a criminal act. Employees should be fully aware of the severe legal and organizational consequences associated with such actions.

6 User Management Policy

6.1 Purpose

The User Management Policy for the Pretense Flip N.V. system establishes the framework for controlling and monitoring user access. Its primary objectives are twofold:

- A. **Prevent Unauthorized Access:** To safeguard the Pretense Flip N.V. system from malicious intrusions and unauthorized entry.
- B. **Enforce Least Privilege:** To ensure that authorized users can only access the resources and perform the functions absolutely necessary for their legitimate job responsibilities.

This policy outlines the Identity and Access Management (IAM) best practices that Pretense Flip N.V. will implement to achieve these critical security controls.

6.2 Scope

This policy applies to **all individuals and entities requiring access to Pretense Flip N.V. data or systems**. This includes, but isn't limited to, employees, contractors, vendors, and any other account holders, regardless of their location or the specific form of access they utilize.

6.3 Logical Access Control Policy²⁸

This policy outlines the principles and requirements for managing logical access to Pretense Flip N.V. systems and data, ensuring that access is granted, maintained, and revoked securely and efficiently.

6.4 User Access Authorization

1. **Principle of Least Privilege:** User access privileges will be granted based strictly on business need and the principle of least privilege. This means users will only have access to the resources and functionalities essential to perform their legitimate job responsibilities.²⁹
2. **Sensitive and Production Environments:** Access to sensitive or production computer resources will be provided only when demonstrably necessary for Pretense Flip N.V. business tasks and is directly tied to an individual's job function.³⁰
3. **Unique User Identifiers:** The use of unauthenticated (i.e., not password-protected) user IDs or user IDs not associated with a single, identified user is strictly prohibited. Every user must have a unique user account identifier and a personal, secret password for access to Pretense Flip N.V. information systems and networks.
4. **System and Application Authentication:** All systems and applications must require authentication using a password or token.

6.5 Access Review and Management³¹

1. **Regular Access Reviews:** User access rights must be regularly reviewed and updated to ensure users maintain the least privileged level of access required for their current roles.
2. **Role-Based Access Control:** Users will only be assigned roles that specifically require privileged access when necessary to perform their job responsibilities.

²⁸ISO 27001 A9 & A9 25

²⁹PCI DSS 7.1

³⁰PCI DSS 7.1.3

³¹PCI Dss8.1.1

3. **System Owner Responsibilities:** Owners of IT systems are responsible for determining appropriate access control rules and rights for each user. They must also clearly specify who has the right and responsibility to create new users and administer their access rights.

6.6 Prohibited Practices³²

Prohibition of Generic Accounts: Generic identities, group identities, and common user accounts are not permitted in production or support environments. Exceptions may be considered for test, experimental, or development environments under strict control and justification.

6.7 VPN WIFI

We must monitor and control all access to our company's Virtual Private Network (VPN) and Wi-Fi networks.³³ This policy outlines the strict procedures to ensure secure, authorized access, protect sensitive information, and maintain the integrity of our systems.

6.7.1 Key Access Requirements³⁴

1. **Authorization from Information System Owner:** Before granting any access, we must get explicit authorization from the owner of the specific information system being accessed. This ensures the individual responsible for the data or system approves the proposed access.³⁵
2. **Management Approval for Access Rights:** On top of system owner approval, we need separate and explicit approval for access rights from Company Management. This dual-approval process adds an extra layer of scrutiny and oversight.
3. **Role-Appropriate Access and Segregation of Duties:** We'll grant access privileges strictly based on the principle of least privilege. This means users only get the minimum access necessary to do their assigned duties. This also aligns with segregation of duties, preventing any single person from having too much control over critical functions.
4. **Pre-Authorization Activation:** We won't activate access rights until all required authorization procedures are fully completed and documented. This prevents premature or unauthorized access to company resources.
5. **Dynamic Access Rights for Role Changes:** If an employee changes roles or job responsibilities within the Company, we'll promptly adapt their access rights to reflect their new duties. This ensures access remains appropriate and revokes any unnecessary privileges from previous roles.
6. **Regular Review of Access Rights:** We'll conduct a regular and systematic review of all access rights in collaboration with the owners of the respective information systems. This ongoing process verifies that access remains appropriate, necessary, and compliant with current policies.
7. **Sanctions for Unauthorized Access:** We'll clearly define and rigorously enforce specific sanctions for unauthorized access to the Company's VPN, Wi-Fi networks, or any information system. These sanctions may include disciplinary action up to and including termination of employment, and potential legal action.

³²PCI DSS 7.1.2

³³ISO 27001 A.9.2.5

³⁴ISO 27001 A.9.2.3

³⁵PCI DSS 8.5

6.7.2 Control of Entry to a System³⁶

Entry to an IT system will be achieved by requiring the would-be user to log on to the system by entering a user ID or user name recognisable by the system, and then a password or passphrase to confirm that they are the legitimate owner of the user ID. Users should not be allowed to communicate with the system in any way before completing log-on.

6.7.2.1 User Identification

A user ID most often consists of a non-secret string of characters and is normally the first thing the user provides the system when attempting to log on and gain access.

For the protection of both the user and the Company, a user ID shall be unique to the user and never shared or known to others, neither during a user's duration with the Company nor thereafter. No one should be granted a user ID for any Company system unless that person has a recognised need to use the system and has been properly identified and authorised.

6.7.2.2 Authentication

Before being allowed to log in to a system and gain access to any resource, the user's identity must be authenticated to prevent impersonation. Whilst passwords will be acceptable on internal networks, these may not suffice for high-risk environments.

In addition to assigning a unique ID, for critical systems, one or more of the following methods should be employed for user authentication:

Something you know, such as a password or passphrase. Something you have, such as a token device or smart card. Something you are, such as a biometric.

6.7.2.3 Authorisation

1. A user or process must be granted the right to access a system. Users with higher levels of privilege may themselves grant access rights to resources under their control to other users or processes. In all cases, the concept of least privilege or "need to know" must be adhered to.
2. Access rights to data files are to be decided strictly on content and the role of the user. In addition, restricting access to other resources such as terminals, printers, and network services must also be considered. It is recommended to restrict the use of system-administrator, security-administrator, database-administrator, and similar commands, to a limited number of users and terminals.
3. The following steps must be taken before authorisation to access any resource is granted: Establish exactly what resources each person or group of people need to access and in what way (eg. READ, WRITE, etc.), taking note of anticipated future needs.
4. Standardise user identifiers and task names: the standardised names should preferably reflect the section of the Company for which the data owner works.
5. Define file and other resource naming standards based on the process, the department/unit, or the individual involved.
6. Standardise user identifiers and task names: the standardised names should preferably reflect the section of the Company for which the data owner works.
7. Define file and other resource naming standards based on the process, the department/unit, or the individual involved.

8. Privileged users should not perform regular business activities using privileged accounts.
9. Privileged access should be granted to individuals only after they read this policy, obtain approval from their direct supervisor, and sign a privileged access agreement form. Gaining and using privileged access should be audited. Individuals with privileged access will take necessary precautions to protect the confidentiality of the information they are accessing. If during the performance of their duties, they are exposed to information that might indicate inappropriate use, they must consult their direct supervisor.

6.7.3 Terminating User Access

1. When an employee or an external contractor is terminated or changes role, all the access rights to information assets must be removed or changed accordingly.³⁷ The employee's account has been closed/disabled.
2. All correspondence must be kept on file, for reference. The data retention period is defined in the Data Retention Policy. Special attention would be given to privileged access rights, for example, system administrators and root accounts.

6.7.4 Miscellaneous Access Controls

6.7.4.1 Dormant and Dead Accounts

1. Dead or inappropriately privileged accounts should not be left on a system because they could provide the vehicle for misuse. Steps to take should include some or all these controls:
2. Removal of vendor's accounts used for setting up the system or changing their passwords since the initial passwords are widely known.
3. Introduction of procedures to allow users to request their access rights be revoked for set periods (such as vacation leave) and subsequently restored.

6.7.4.2 Automatic Lockout (Screen Lock)

1. The automatic disablement of logged-on workstations after a period of inactivity shall be implemented either through group policy or by the employees themselves. This feature must be implemented on laptops (when applicable).
2. The user should be able to manually invoke the screen lock program.

6.7.4.3 Unsuccessful Login Attempts

1. The login procedure should lock out a person who has input an incorrect password after a predetermined number of times.
2. The number of attempts permissible before logout should be between 3 to 6, depending on the risk rating of the system or information being accessed.
3. The user should not be enabled unless properly authenticated. Automatic re-enabling should not be permitted.

6.8 Compliance

Violation of this policy should be avoided. If deviations are necessary, these must be approved by top management, and the rationale behind the authorisation to deviate should be documented.

Employees should report any misuse or abuse of authorisation levels or user accounts or any cases of suspected unauthorised access. Should an employee have access to resources and is aware that s/he should not have access to such resources, s/he should report it and refrain from using these access rights. Failure to do so will be treated as a violation of this policy.

7 Communication Security Policy

7.1 Purpose of This Policy

This policy outlines the rules for using the Company's email systems and other digital communication services. Our email systems are primarily for conducting Company business. This policy applies to all electronic messages sent or received, whether through our internal networks or external services the Company uses.

7.2 Company Ownership of Data

1. All email accounts, equipment, and messages created, sent, or received using the Company's email system are the property of the Company.
2. The Company reserves the right to access, review, and disclose the contents of all messages on its email system to relevant parties or authorities, as deemed necessary and legally permissible.

7.3 Proper Email Usage

1. All email communication must be treated with the same professionalism and care as any other official business communication (e.g., letters, faxes, memos).
2. Sensitive Data: Do not send sensitive or confidential Company data (including in attachments) to clients or colleagues over the Internet without proper encryption or secure methods.
3. Copyright and Proprietary Information: Do not distribute copyrighted or proprietary information via Company email unless a director has given explicit written approval.
4. Prohibited Content: Do not use Company email for:
 - A. Commercial messages unrelated to Company business.
 - B. Employee solicitations.
 - C. Messages of a religious or political nature.
 - D. Bulk forwarding of jokes, chain letters, or similar non-business materials, especially to external recipients.
 - E. Content that is or could be considered offensive, disruptive, harassing, or discriminatory. This includes, but is not limited to, obscene language or images, and comments or images related to race, ethnicity, sex, or gender.
5. **Virus Warnings:** If you receive an urgent virus warning, do not forward it. Instead, report it immediately to the Internal IT Team for verification, as many such warnings are hoaxes.
6. **Unauthorized Access to Emails:** Employees may not retrieve or read an email not addressed to them unless specifically authorized by the Company or the intended recipient.
7. **Malware Scans:** All email attachments and downloads must be scanned for malware before opening or using them.

7.4 Non-Business Email Use

Occasional and incidental personal use of Company email is permitted. However, any such personal messages become the property of the Company and are subject to all the conditions outlined in this policy, including the Company's right to access and disclose their contents.

7.5 Network Security Management

The Company maintains robust security measures for its networks.

Network Ownership and Accountability: The Company will designate an owner for each network segment. This owner is responsible for enforcing security procedures for their assigned network.

Network Protection: Our internal networks are protected by firewalls and intrusion detection systems to prevent unauthorized access and detect suspicious activity.

Network Segmentation: Operational networks (those vital for day-to-day business) are kept separate from support, development, and test networks to minimize risks.³⁸

Logging and Monitoring: All actions that could affect information security on our networks are logged and continuously monitored for suspicious or unauthorized activity.

Restricted Access: Only authorized users are permitted to connect and access systems on our network.

7.6 Security of Network Services³⁹

1. All services running on our network must be secured.
Service Examples: This includes, but is not limited to, services like Firewalls, Intrusion Detection Systems (IDS), DNS, DHCP, FTP, and SMTP.
2. Service Provider Review: The Company will regularly evaluate and review the ability of our network service providers to securely manage the services they provide.
3. By adhering to this policy, you help protect the Company's valuable information and ensure a secure communication environment for everyone. If you have any questions or require clarification on this policy, please contact your manager or the IT Department.

³⁸ISO 27001 A.13.1.3

³⁹ISO 27001 A.13.1.2

8 Corporate Media Handling Policy

8.1 Purpose

This policy establishes the requirements for the secure handling, storage, transfer, and disposal of all media containing Company information, with particular emphasis on sensitive and confidential data, including but not limited to Cardholder Data (CHD) as defined by the Payment Card Industry Data Security Standard (PCI DSS). The primary objective is to prevent unauthorized disclosure, modification, loss, destruction, or unauthorized access to information, thereby ensuring the confidentiality, integrity, and availability of Company assets in compliance with ISO/IEC 27001 and PCI DSS.

8.2 Scope

This policy applies to all employees, contractors, temporary staff, and any third parties who access, handle, store, or dispose of Company media, regardless of format (physical or electronic), and all types of media used for storing Company information. This includes, but is not limited to, hard drives, solid-state drives, USB drives, CDs, DVDs, backup tapes, memory cards, paper documents, faxes, and any other data storage devices or physical records.

8.3 Definitions

1. **Media:** Any physical or electronic material capable of storing data, including but not limited to paper, magnetic tapes, optical discs, hard disk drives, solid-state drives, USB flash drives, and mobile devices.
2. **Sensitive Information:** Any information classified as confidential, restricted, or secret according to the Company's Data Classification Policy, including but not limited to Personally Identifiable Information (PII), Cardholder Data (CHD), intellectual property, trade secrets, and financial data.
3. **Cardholder Data (CHD):** At a minimum, the full Primary Account Number (PAN). CHD also includes the cardholder name, expiration date, and service code when stored with the PAN.
4. **Disposal:** The permanent removal of data from media such that it cannot be recovered or reconstructed.
5. **Sanitization:** The process of rendering data unrecoverable from media using methods such as degaussing, physical destruction, or cryptographic erasure, in accordance with industry best practices (e.g., NIST SP 800-88 Guidelines for Media Sanitization).

8.4 Policy Statements

8.4.1 General Principles for Media Management ⁴⁰

1. Data Classification Integration: All media containing Company information shall be handled in accordance with the Company's Data Classification and Handling Policy. The security controls applied to media shall be commensurate with the classification of the data it contains.
2. Business Justification: The use, storage, and transfer of all media, especially removable media and hardcopy materials containing sensitive information, must be justified by a legitimate business need and approved by the relevant Data Owner or designated authority.

⁴⁰ISO 27001 A.8.3.1

3. Secure Storage: All media containing Company information shall be stored in secure environments that protect against unauthorized access, damage, theft, and environmental hazards (e.g., temperature, humidity, fire, water), in accordance with manufacturer specifications and industry best practices.
4. Access Control: Access to stored media shall be restricted to authorized personnel on a 'need-to-know' and 'least privilege' basis, ensuring appropriate physical and logical access controls are in place.
5. Inventory and Tracking⁴¹: An accurate inventory of all stored electronic and hardcopy media containing sensitive or confidential information shall be maintained. This inventory shall be reviewed and verified at least annually by the Internal IT Team or designated personnel. The log shall include details such as media type, location, owner, date created, and classification.
6. Encryption: Where data classification dictates (e.g., for sensitive or confidential data, especially CHD), encryption shall be applied to data stored on media, both at rest and in transit, in accordance with the Company's Encryption Policy and PCI DSS requirements.
7. Media Degradation: To mitigate data degradation and potential loss, critical data stored on media shall be periodically transferred to fresh media before data integrity is compromised. This refresh cycle shall be determined based on media type and data criticality.

8.4.2 Management of Removable Media ⁴²

1. Restricted Usage: The use of removable media is strictly limited to justified business reasons.
2. Isolation of Work and Personal Media: The same removable media (e.g., USB drives) must not be used for both Company work and personal computing activities to mitigate the risk of malware transfer or unauthorized data exfiltration.
3. Authorization for Removal: Prior authorization from the relevant Data Owner or the Internal IT Team is mandatory for any removable media containing Company information to be removed from Company premises. Such removals shall be logged, including details of the media, data classification, purpose of removal, and authorized personnel.
4. Security during Transit: Refer to Section 8.4.6 for requirements regarding secure transport of media.
5. Logging: A detailed log of all issued and returned removable media shall be maintained to ensure an auditable trail.

8.4.3 Hardcopy Media Handling ⁴³

1. Restricted Movement: Printed reports or materials containing sensitive or confidential information (e.g., CHD, PII) are strictly prohibited from being removed from any designated secure Company office environment, data center, or computer room without prior documented authorization from the Internal IT Team and the relevant Data Owner.
2. Secure Retention: Hardcopy materials containing sensitive or confidential data shall be physically retained, stored, or archived only within secure Company office environments or designated secure storage facilities. Retention periods shall be aligned with legal, regulatory, and business requirements, ensuring storage only for the minimum necessary time.

⁴¹ PCI DSS 9.9⁴²ISO 27001 A.8.3.1 &⁴³PCI DSS 9.6

3. Clear Labelling: All hardcopy material containing confidential or sensitive information must be clearly labelled as such (e.g., "CONFIDENTIAL," "INTERNAL USE ONLY," "PCI DSS SENSITIVE").
4. Secure Storage Containers: All confidential or sensitive hardcopy media must be stored in secure and locked containers (e.g., lockers, cabinets, desks, storage bins) approved by the Internal IT Team.
5. Prohibited Storage: Confidential or sensitive hardcopy material shall never be stored in unlocked or insecure containers, open workspaces, or publicly accessible areas.
6. Shredding and Disposal: Refer to Section 8.4.5 for specific requirements on hardcopy media disposal.

8.4.4 Electronic Media Handling⁴⁴

1. Authorization for Copying: Sensitive or confidential information must never be copied onto removable electronic media without explicit, documented authorization from the relevant Data Owner or the Internal IT Team.
2. Restricted Movement: Electronic media containing sensitive or confidential information is strictly prohibited from being removed from any designated secure Company office environment, data center, or computer room without prior documented authorization from the Internal IT Team. Exceptions are permissible only for officially approved and secured computer system backups transferred as per Section 8.4.6.
3. Secure Retention: Electronic media containing consumer confidential or sensitive data shall be physically retained, stored, or archived only within secure Company office environments or designated secure storage facilities. Retention periods shall be aligned with legal, regulatory, and business requirements, ensuring storage only for the minimum necessary time.
4. Clear Labelling: All electronic media containing confidential or sensitive information must be clearly labelled as such (e.g., "CONFIDENTIAL," "PCI DSS SENSITIVE").
5. Secure Storage: All removable electronic media containing confidential or sensitive data must be stored securely, protected against unauthorized access, damage, or loss.

8.4.5 Media and Equipment Destruction & Sanitization⁴⁵

1. Formal Procedures: The Company shall implement formal, documented procedures for the secure and irreversible disposal or sanitization of all media (hardcopy and electronic) that are no longer needed. These procedures shall differentiate based on media type and data classification.
2. Irrecoverability: Upon disposal or sanitization, the Company shall ensure that information stored on the media cannot be recovered or reconstructed, even with advanced forensic techniques.

⁴⁴PCI DSS 9.6,9.9⁴⁵ISO 27001 A 8.3.2 &PCI DSS9.8

3. Disposal Log: A comprehensive log of all media disposal and sanitization activities shall be maintained to provide an audit trail. This log shall include:
 - a) Date of disposal/sanitization.
 - b) Type of media.
 - c) Serial number or unique identifier (if applicable).
 - d) Classification of data previously held.
 - e) Method of disposal/sanitization.
 - f) Name of personnel performing the activity.
 - g) Verification of successful sanitization (if applicable).
4. Hardcopy Material Disposal⁴⁵: Hardcopy materials containing sensitive information (e.g., CHD, PII) shall be disposed of through cross-cut shredding, incineration, pulping, or other approved methods that render the information unrecoverable.
5. Dedicated Disposal Containers: Specially dedicated and secured storage containers (e.g., locked shred bins) shall be used for media awaiting destruction to prevent unauthorized access to their content prior to final disposal.
6. Electronic Media Sanitization/Destruction⁴⁶: Electronic media containing sensitive information shall be sanitized or destroyed using secure methods (e.g., degaussing, cryptographic erasure, physical destruction) that render the data unrecoverable.
7. Disposal of Equipment⁴⁵: Before any equipment containing data storage components (e.g., hard drives, SSDs) is removed from the Company's network, redeployed, sold, or disposed of, the data storage components must be sanitized or physically destroyed to ensure no information can be recovered. This includes equipment used by third parties on behalf of the Company.

8.4.6 Physical Media Transfer ⁴⁷

1. Protection During Transport: Media containing Company information, particularly sensitive or confidential data, must be adequately protected against unauthorized access, theft, and damage during transport. This includes using secure, tamper-evident packaging.
2. Reliable Transport Mechanisms ⁴⁸: When media is transported off-site, reliable transport methods must be used that allow for accurate tracking, confirmation of secure delivery, and protection from unauthorized access. This may include secured courier services or dedicated Company transport with appropriate security measures. All media couriers and transport mechanisms must be certified or approved by the Internal IT Team.

⁴⁵PCI DSS 9.8.1⁴⁶PCI DSS 9.8.2⁴⁷ISO 27001 A 8.3.3⁴⁸PCI DSS 9.6.2

3. Logging of Transfers ⁴⁹: A comprehensive log shall be maintained for all media transfers from one location to another. The log shall document:
 - a) Date and time of transfer.
 - b) Type and quantity of media.
 - c) Data classification.
 - d) Origin and destination.
 - e) Name of personnel initiating the transfer.
 - f) Name of personnel receiving the media (with signature for confirmation of receipt).
 - g) Transport method used.
4. Authorization for Transfer: All media transport or transfer, especially for sensitive or confidential data, must be authorized by the relevant Data Owner prior to movement.
5. Jurisdictional Compliance: For media moved across jurisdictional borders, legal advice shall be sought to ensure compliance with relevant data protection laws and regulations (e.g., local data residency laws).

8.4.7 Backup Management ⁵⁰

1. Regular Backups: Backups of critical data, software, and system images shall be taken regularly in accordance with the Company's Backup and Recovery Policy to protect valuable information against loss or corruption.
2. Backup Plan: A comprehensive backup plan shall be maintained, specifying:
 - a) Systems and data covered by backups.
 - b) Backup frequency (e.g., daily, weekly, monthly).
 - c) Retention periods for backups.
 - d) Secure storage locations for backup media (on-site and off-site).
 - e) Encryption requirements for backup media containing sensitive data.
3. Monitoring and Testing: The execution of backup procedures shall be regularly monitored to ensure successful completion. Backup media and recovery procedures shall be periodically tested to verify data integrity and the ability to restore systems and data effectively.
4. Secure Off-Site Storage: Offline storage media utilized for archival or backup purposes must be handled and retained in a secured environment, with access restricted solely to authorized Company personnel and approved contracted storage facility personnel.

8.5 Roles and Responsibilities

1. Internal IT Team: Responsible for implementing, maintaining, and monitoring the technical controls related to media handling, conducting inventories, approving disposal methods, and managing secure transport mechanisms.
2. Data Owners: Responsible for classifying data, authorizing the use, transfer, and copying of sensitive data onto media, and determining retention periods.
3. All Employees/Contractors: Responsible for adhering to this policy in all their activities involving Company media. Reporting any suspected policy violations or incidents immediately.

⁴⁹PCI DSS 9.6.2⁵⁰ISO 27001 A 8.3.1 &
A 12.3.1

4. Management: Responsible for ensuring adequate resources are available for policy implementation and enforcement.

8.6 Training and Awareness

All employees and relevant third parties shall receive mandatory training on this Media Handling Policy, the Company's Data Classification Policy, and related security procedures. Awareness campaigns will be conducted periodically to reinforce understanding and compliance.

8.7 Policy Enforcement

Any violation of this policy may result in disciplinary action, up to and including termination of employment or contract, and may also lead to legal action where applicable. Non-compliance with PCI DSS requirements can result in significant fines and reputational damage.

8.8 Review and Updates

This policy shall be reviewed at least annually, or more frequently if there are significant changes to Company operations, technology, legal or regulatory requirements (e.g., updates to PCI DSS or ISO 27001).

9 Information Classification and Handling Policy

9.1 Purpose

Data is one of our company's most valuable assets, demanding responsible and ethical use. This policy establishes a framework for classifying company data, implementing appropriate security measures, and assigning clear responsibilities for data handling. This ensures all data is protected effectively.

9.2 Data Roles and Responsibilities⁵¹

9.2.1 Data Owners

1. Data Owners are accountable for:
 - a) Understanding and classifying all data under their ownership.
 - b) Ensuring adequate security measures are applied to their data, consistent with its classification and all legal requirements.
 - c) Authorizing individuals' access to the data and defining their access rights.
2. Management will appoint Data Owners and Custodians based on a clear understanding of the data and individual roles. While the company retains overall ownership of data, responsibility and authority will be delegated to relevant departments or authorities as needed. This acknowledges that data ownership is not a monolithic concept but rather a set of defined responsibilities.

9.2.2 Data Custodians/Processors

Data Custodians are responsible for safeguarding data entrusted to them, regardless of its format, for specified periods. They must ensure that the required level of security to protect the data is maintained throughout their custodianship. The Internal IT Team is an example of a Data Custodian.

9.2.3 Data Users

Data Users are granted access rights by Data Owners to perform their duties. Users must not abuse these rights and may only access and use data as explicitly authorized by the Data Owners.

9.3 Data Classification Standards⁵²

This policy outlines the data classification standards, the responsibilities of employees in adhering to these standards, and provides guidelines for information classification.

9.3.1 Objective

1. To ensure all information receives an appropriate level of protection commensurate with its importance to the company.⁵²
2. Information is classified based on legal requirements, value, criticality, and sensitivity. Procedures for information labelling must be developed and implemented in accordance with the following classifications:
3. Confidential Data: This applies to our most sensitive business information, strictly for internal company use. Unauthorized disclosure could severely and adversely impact the company, business partners, and/or customers. Examples include password encryption keys, cardholder information, bank account details, intellectual property, and market research audit reports.

⁵¹ISO27001 A 8.2

⁵²ISO27001 A 8.2.43

4. PCI Data: A specialized category of confidential data, this refers to credit card and transaction data requiring protection under the Payment Card Industry (PCI) Data Security Standard (DSS).
 - a) Cardholder Data: May be stored after transaction authorization. Includes:
 - i. Primary Account Number (PAN)
 - ii. Cardholder Name
 - iii. Service Code
 - iv. Expiration Date
 - b) Sensitive Authentication Data: Must not be stored after transaction authorization. Includes:
 - i. Full Track Data (CAV2/CVC2/CVV2/CID)
 - ii. PIN/PIN Block
 - c) Private Data: Applies to personal information intended for internal company use. Unauthorized disclosure could adversely impact the company and/or its employees. Examples include policies and procedures, procedure metrics, human resources information, and meeting minutes.
 - d) Public Domain Data: Encompasses all other information that does not fit into the above classifications. Unauthorized disclosure is not expected to seriously or adversely impact the company. Any release of this information must be authorized by the COO or CEO. Examples include news articles and marketing campaigns.
5. When aggregating data, the classification should be based on the most secure classification level present. If data of mixed classifications exists within the same file, report, or memorandum, the overall classification of that document should be the highest level.

9.4 Labelling of Information⁵³

Procedures for information labelling must be developed and implemented in accordance with the information classification scheme. Labels should be easily recognizable and practical, covering both physical and electronic formats. These procedures will guide when and how labels are attached, considering how information is accessed. All employees and contractors must be made aware of these labelling procedures.

9.5 Data Access⁵⁴

All confidential or sensitive data must be protected by access controls to prevent improper disclosure, modification, deletion, or unavailability. All access rights to information and systems must be recorded.

Access rights are configured on a "deny all but what is needed" basis, meaning users only have access to information essential for their business role. Requests to access systems or applications handling confidential, sensitive, or private information must follow the established data access request process. All changes to user access rights require approval from the Internal IT Team.

Access to data exceeding an employee's authorized role also requires following the data access request process and must include documented limits, such as access source and time limits.

⁵³ISO27001 A 8.2.2

⁵⁴ISO27001 A 8.2.43

All Pretense Flip N.V. applications that process or retrieve cardholder information must be configured to mask or truncate displayed PANs, showing a maximum of the first six and last four digits. If an application's specific purpose requires displaying the full PAN, approval must be obtained from the Internal IT Team during the Requirements Phase, as described in the Software Development Policy. In all cases, displaying full or masked PANs must be limited to the fewest possible users, and only personnel with a legitimate business need can view more than the first six and last four digits of the PAN.

9.6 Technical Measures to Protect Data

The company sets rules for protecting each asset type according to its confidentiality level.

Technical Measures:

1. **Public Domain Data:** Requires no specific protection during storage or transmission.
2. **Private Data:**
 - a) Availability and integrity must be protected during transmission and storage.
 - b) Systems housing and carrying such data must be securely configured, and message authentication must be used during transmission.
 - c) Adequate backups of this data must be regularly taken and stored both on-site and off-site.
 - d) If transmitted over a public network, it must be encrypted to preserve confidentiality.
3. **Confidential Data:**
 - a) Access must be strictly on a need-to-know/least privilege basis.
 - b) Such data must always be transmitted in an encrypted format.
4. **PCI Data:**
 - a) Must be afforded the highest levels of control.
 - b) Encryption must be employed during storage and transmission using the strongest available techniques.
 - c) Networks or databases housing such information should be segregated from other networks.
 - d) Media Classification
 - e) Physical media containing classified information shall be identified visually using appropriate stickers, labels, or markers to denote its confidentiality level.

10 Data Retention Policy

10.1 Purpose

This policy outlines the principles and procedures for the retention and secure disposal of all data, with particular emphasis on sensitive and confidential information, including Cardholder Data (CHD), stored on Pretense Flip N.V. networks and systems. Its aim is to ensure compliance with legal, regulatory, and business requirements, including those of ISO 27001 and PCI DSS, while minimizing the risks associated with excessive data retention.

Exemptions from this policy will be permitted only if approved in advance and in writing by the **Chief Technology Officer (CTO)** and documented with a clear business justification and associated risk assessment.

10.2 Scope

This policy applies to all data, regardless of format (electronic or physical), generated, collected, processed, or stored by Pretense Flip N.V., whether on company-owned systems, third-party services, or employee-owned devices. This includes, but is not limited to, production data, backup data, logs, and any other information classified as sensitive or confidential.

10.3 Principles of Data Retention⁵⁵

All data, particularly sensitive and confidential information, will be retained only for as long as is necessary to fulfil its original purpose, meet legal or regulatory obligations, or satisfy legitimate business requirements.

The specific retention period for each data type will be established and documented by the **Data Owner**, in consultation with Legal, Compliance, and IT teams, and aligned with the Information Classification and Handling Policy.

Key principles include:

- a) **Data Minimization:** Retain the minimum amount of data for the shortest possible duration.
- b) **Legal & Regulatory Compliance:** Adhere to all applicable laws, regulations, and industry standards (e.g., Data Protection Law / Legislation, local tax laws, PCI DSS).
- c) **Business Necessity:** Retain data only when there is a clear and documented business need.
- d) **Secure Disposal:** Ensure all data is securely and irrecoverably disposed of once its retention period expires.
- e) **Accountability:** Assign clear responsibilities for data retention and disposal.

10.4 Data Retention Schedule

Pretense Flip N.V. will maintain a comprehensive **Data Retention Schedule** that specifies:

- a) **Data Category/Type:** A clear description of the data (e.g., Customer PAN, Transaction Logs, Employee Records, Contractual Agreements).
- b) **Data Owner:** The designated individual or department responsible for the data.
- c) **Retention Period:** The defined length of time the data must be retained (e.g., 7 years, 90 days, immediately after authorization).

- d) **Justification:** The legal, regulatory, or business reason for the specified retention period.
- e) **Disposal Method:** The approved secure method for disposal (e.g., cryptographic erasure, physical shredding, degaussing).
- f) **Review Cycle:** Frequency for reviewing the retention period and justification.

*Initial data types and their proposed retention periods should be listed here or in an appended schedule.
Example:*

Data Category	Data Owner	Retention Period	Justification	Disposal Method	Review Cycle
Financial Records	Finance	7 years	Tax/Accounting Regulations	Secure Erasure/Shredding	Annually
Customer PAN (stored)	Sales	As per PCI DSS (see below)	Business Need (e.g., recurring billing)	Strong Cryptography	Quarterly
Audit Logs (PCI related)	IT	1 year (90 days accessible)	PCI DSS Req. 10.7	Secure Erasure	Annually
Employee HR Records	HR	Legal requirement (e.g., 5 years post-employment)	Labor Laws	Secure Erasure/Shredding	Bi-annually
Marketing Leads	Marketing	12 months (no activity)	Business Need	Secure Erasure	Annually

10.5 PCI DSS Requirements for Data Retention & Disposal

As a critical component of Pretense Flip N.V.'s payment card processing, specific requirements for Cardholder Data (CHD) and Sensitive Authentication Data (SAD) apply:

10.6 Prohibited Data Retention⁵⁵

1. Pretense Flip N.V. **will not store** Sensitive Authentication Data (SAD) after authorization. This includes:
 - a) Full contents of any track (magnetic stripe or chip equivalent data).
 - b) Card Verification Value (CVV2, CVC2, CAV2, CID) or value (the three- or four-digit number printed on the front or back of a payment card).
 - c) PINs or PIN blocks.

⁵⁵PCI DSS 3.2

2. If SAD is received during the authorization process, it must be rendered **unrecoverable** upon completion of authorization.

10.7 Permitted Data Retention & Protection ⁵⁶

1. **Primary Account Number (PAN):** If stored, the PAN **must be rendered unreadable** anywhere it is stored (including databases, backups, logs, paper, and portable digital media) using one of the following methods:
 - a) Strong one-way hash functions (hashed indexes) with an associated salt.
 - b) Truncation (removing a segment of PAN, e.g., only storing the first six and last four digits).
 - c) Index tokens and pads (pads must be securely stored).
 - d) Strong cryptography with associated key management processes and procedures.
2. **Limited PAN Display⁵⁷:** When displayed, the PAN must be masked. The first six and last four digits are the maximum number of digits to be displayed. Only personnel with a legitimate documented business need can view more than the first six and last four digits of the PAN, and such access must be strictly controlled and logged.
3. **Other Cardholder Data⁵⁷:** Cardholder Name, Service Code, and Expiration Date may be stored if there is a documented business need, provided they are adequately protected in accordance with PCI DSS Requirement 3.

10.8 Data Sources & Retention Specifics (PCI DSS)

1. **Incoming Transaction Data:** Only elements of CHD permitted for storage (e.g., truncated/masked PAN, expiration date, name) will be retained as per business requirements. SAD will be immediately purged.
2. **All Logs⁵⁸:** Audit logs for all system components in scope for PCI DSS must be retained for at least **one year**. At least the last **three months' logs must be immediately available** for online analysis.
3. **History Files, Trace Files, Database Schema, Database Contents:** Retention of these data sources must align with the overall data retention schedule, with particular attention to any embedded CHD or SAD, which must be protected or purged according to PCI DSS.
4. **Secure Disposal of Cardholder Data (Requirement 3.1)**

Pretense Flip N.V. will implement processes for the secure deletion or rendering unrecoverable of stored Cardholder Data when it is no longer needed for legal, regulatory, or business purposes. This process will be verified at least quarterly to ensure that stored CHD exceeding the defined retention period has been securely deleted or rendered unrecoverable.

⁵⁶PCI DSS 3.3 & 3.4

⁵⁷PCI DSS 3.3.1

⁵⁸PCI DSS 10.7

11 Cryptographic Policy⁵⁹

11.1 Purpose

This Cryptographic Policy outlines Pretense Flip N.V.'s principles, requirements, and responsibilities for the effective and secure use of cryptography to protect information and systems. Its primary objective is to safeguard the confidentiality, integrity, and authenticity of Pretense Flip N.V.'s data, particularly sensitive and confidential information, including Cardholder Data (CHD), in compliance with legal, regulatory, and contractual obligations, most notably ISO 27001:2022 and the Payment Card Industry Data Security Standard (PCI DSS).

11.2 Scope

This policy applies to all Pretense Flip N.V. personnel (employees, contractors, temporary staff), systems, applications, data (in all states: at rest, in transit, in use), and processes where cryptography is employed or required. This includes, but is not limited to:

1. Protection of Cardholder Data (CHD) and Sensitive Authentication Data (SAD).
2. Protection of other sensitive and confidential information as defined by Pretense Flip N.V.'s Information Classification and Handling Policy.
3. Secure communication channels (internal and external).
4. Data storage (on-premises and cloud).
5. Authentication mechanisms.
6. Software development and deployment.
7. System and application logs.
8. Backups and archives.

11.3 Guiding Principles

Pretense Flip N.V.'s use of cryptography is guided by the following principles:

1. **Risk-Based Approach:** Cryptographic controls will be applied based on the classification and criticality of the information and systems being protected, as identified through Pretense Flip N.V.'s risk assessment process.
2. **Compliance:** All cryptographic implementations will comply with relevant legal, regulatory, and contractual requirements, including PCI DSS and ISO 27001.
3. **Effectiveness:** Only strong, industry-standard, and cryptographically sound algorithms, protocols, and key lengths will be used.
4. **Key Management:** Robust and secure key management practices are paramount to the effectiveness of any cryptographic solution.

⁵⁹ISO 27001 A10

5. **Auditability:** Cryptographic implementations and key management processes will be designed to allow for proper auditing and monitoring.
6. **Segregation of Duties:** Where feasible, responsibilities related to cryptographic functions (e.g., key generation, storage, usage, destruction) will be separated to prevent single points of failure or compromise.

11.4 Cryptographic Requirements

11.4.1 Information Classification and Cryptography Linkage

The application of cryptographic controls will be directly correlated with the information classification level, as defined in Pretense Flip N.V.'s Information Classification and Handling Policy:

1. **Public Domain Data:** Generally, no specific cryptographic protection is required.
2. **Private Data:** Encryption for data in transit over untrusted networks (e.g., public internet) is required. Encryption at rest is highly recommended for critical systems housing such data.
3. **Confidential Data: Must be encrypted both in transit and at rest.** This includes sensitive business information, intellectual property, financial data, and personal employee data.
4. **PCI Data (Cardholder Data Environment - CDE): Mandatory encryption both in transit and at rest** for all Primary Account Numbers (PAN) and other protected CHD. Strict adherence to PCI DSS cryptographic requirements is non-negotiable.

11.4.2 Approved Cryptographic Algorithms and Protocols

Only the following cryptographic algorithms, protocols, and key lengths are approved for use within Pretense Flip N.V.'s environment. Any deviation requires explicit written approval from the **CTO** and justification based on a risk assessment.

1. **Symmetric Encryption (for Data at Rest and Bulk Data Encryption):**
 - a) **Algorithm:** AES (Advanced Encryption Standard)
 - b) **Key Length:** Minimum 256-bit (e.g., AES-256)
2. **Asymmetric Encryption (for Key Exchange, Digital Signatures, Authentication):**
 - a) **Algorithms:** RSA, ECC (Elliptic Curve Cryptography)
 - b) **Key Lengths:**
 - I. RSA: Minimum 2048-bit (preferably 3072-bit or higher)
 - II. ECC: Minimum 256-bit (e.g., NIST P-256, P-384, P-521)
3. **Hashing Algorithms (for Integrity, Digital Signatures, Password Hashing):**
 - a) **Algorithms:** SHA-2 (SHA-256, SHA-384, SHA-512)
 - b) **Deprecated/Prohibited:** MD5, SHA-1 (unless used in legacy systems with compensating controls and a documented remediation plan).
4. **Secure Communication Protocols (for Data in Transit):**

- a) TLS (Transport Layer Security): Version 1.2 or higher (TLS 1.3 preferred). SSL/TLS 1.0, 1.1 are prohibited.
 - b) IPsec (Internet Protocol Security): For VPNs and network layer encryption.
 - c) SSH (Secure Shell): Version 2 for secure remote access and file transfer. SSHv1 is prohibited.
5. **Password Hashing:** Strong, computationally intensive, salted hashing algorithms (e.g., Argon2, bcrypt, scrypt) are required for all password storage. Simple hashing (e.g., SHA-256) without salt and iteration is prohibited for passwords.

11.4.3 Cryptographic Key Management⁶⁰

Pretense Flip N.V. will implement a robust Cryptographic Key Management System (CKMS) that covers the entire lifecycle of cryptographic keys. This includes:

1. **Key Generation:** Keys must be generated using cryptographically strong random number generators.
2. **Key Storage:**
 - a) Keys must be stored securely, protected from unauthorized access, modification, or disclosure (e.g., Hardware Security Modules (HSMs), Key Management Service (KMS), encrypted key files).
 - b) Access to keys must be on a strict need-to-know and least privilege basis.
 - c) PCI DSS Requirement 3.6 specifically mandates that cryptographic keys used for PAN encryption are protected from disclosure and misuse, including segregation of duties and dual control where appropriate.
3. **Key Distribution:** Secure methods must be used for key distribution, ensuring confidentiality and integrity during transit.
4. **Key Usage:** Keys must only be used for their intended purpose and by authorized entities. Key usage should be logged.
5. **Key Rotation/Change:** Keys must be periodically rotated or changed in accordance with their sensitivity, usage, and industry best practices.
6. **Key Revocation:** A process must be in place to revoke compromised or no longer valid keys immediately.
7. **Key Recovery:** Secure procedures for key recovery (e.g., for data decryption in case of key loss) must be implemented, ensuring authorized access only.
8. **Key Destruction:** Keys must be securely and irrecoverably destroyed when they are no longer needed (e.g., when the data they protect is permanently deleted, or a new key replaces them). This applies to all copies of the key.
9. **Key Management System (KMS):** A dedicated KMS or equivalent mechanism will be utilized to automate and centralize key management processes where feasible.

11.4.4 PCI DSS Specific Cryptographic Requirements

In addition to the above, the following specific PCI DSS requirements regarding cryptography must be strictly adhered to:

1. **Encryption of PAN at Rest⁶¹:** All stored Primary Account Numbers (PAN) must be rendered unreadable using strong cryptography (refer to Section 5.2 of the Data Retention Policy for methods).
2. **Encryption of PAN in Transit⁶²:** PAN must be encrypted during transmission over open, public networks (e.g., the Internet) using strong cryptography.
3. **Key Management for PAN Encryption⁶³:** Robust key management processes must be implemented for cryptographic keys used to encrypt PAN, including:
 - a) Minimizing the number of individuals with access to keys.
 - b) Storing keys in the fewest possible locations.
 - c) Strong access controls to key storage.
 - d) Separation of duties for key management functions.
 - e) Dual control for sensitive key operations.
 - f) Secure key generation, distribution, storage, usage, archiving, and destruction.
4. **No Storage of SAD⁶⁴:** As per the Data Retention Policy, Sensitive Authentication Data (SAD) must not be stored after authorization. If SAD is transmitted, it must be protected with strong cryptography.

11.5 Application of Cryptography

11.5.1 Data at Rest Encryption

1. **Full Disk Encryption:** Required for all laptops, mobile devices, and sensitive servers where data is stored directly.
2. **File-level/Folder-level Encryption:** Employed for specific sensitive files or folders on shared drives or cloud storage.
3. **Database Encryption:** Sensitive data within databases (e.g., PAN, PII) must be encrypted using native database encryption, Transparent Data Encryption (TDE), or application-layer encryption.
4. **Backup and Archive Encryption:** All backups and archives containing confidential or PCI data must be encrypted using strong cryptographic methods.

11.5.2 Data in Transit Encryption

1. All communication over untrusted networks (e.g., public internet) involving confidential or PCI data must use approved secure communication protocols (e.g., TLS 1.2+, IPsec VPNs).
2. Internal network communication deemed sensitive will also utilize encryption where appropriate (e.g., between CDE segments).

⁶¹PCI DSS 3.4⁶²PCI DSS 4.1⁶³PCI DSS 3.5 & 3.6⁶⁴PCI DSS 3.2

11.5.3 Digital Signatures and Hashes

1. Digital signatures will be used to ensure the authenticity and integrity of critical documents, software, and communications where non-repudiation is required.
2. Hashing algorithms will be used for verifying data integrity, storing password hashes, and generating unique identifiers where appropriate.

11.6 Roles and Responsibilities

1. **Chief Technology Officer (CTO):** Overall responsibility for the approval and oversight of this Cryptographic Policy.
2. **Information Security Officer (ISO):** Responsible for developing, implementing, and maintaining this policy, ensuring its alignment with ISO 27001 and PCI DSS, and advising on cryptographic best practices.
3. **Internal IT Team/Security Operations:** Responsible for the implementation, configuration, and day-to-day management of cryptographic controls, key management systems, and monitoring cryptographic usage.
4. **Data Owners:** Responsible for identifying data requiring cryptographic protection based on its classification and criticality.
5. **Application Development Team:** Responsible for incorporating cryptographic requirements into software design, development, and testing, using approved cryptographic libraries and APIs.
6. **All Employees and Contractors:** Responsible for adhering to this policy in their daily activities, including proper handling of encrypted data and cryptographic keys.

11.7 Policy Enforcement

Non-compliance with this Cryptographic Policy may result in disciplinary action, up to and including termination of employment or contract. Additionally, violations may lead to severe legal, regulatory, and financial penalties for Pretense Flip N.V..

11.8 Policy Review

This Cryptographic Policy will be formally reviewed at least **annually**, or more frequently if there are significant changes to:

1. Legal or regulatory requirements (e.g., new PCI DSS versions, data protection laws).
2. Industry best practices or cryptographic standards.
3. Known vulnerabilities in cryptographic algorithms or implementations.
4. Pretense Flip N.V.'s business operations or technology infrastructure.

12 Encryption Policy

12.1 Purpose

This policy outlines the mandatory encryption standards for all applicable mechanisms and systems across Pretense Flip N.V. networks, encompassing those managed by employees and third-party vendors. It also governs the management of encryption keys, including those shared with customers for confidential information exchange. Any documentation provided to customers for key exchange must incorporate these guidelines. Exemptions to this policy require prior written approval from the Chief Technology Officer (CTO).

12.2 Key Management and Access

Encryption keys must be generated, accessed, distributed, and stored in a controlled and secure manner. Access to key components is restricted solely to authorized custodians whose job functions necessitate such access. The CTO is the sole approver for granting key access, and all access requests must be documented on an Authorization Request Form, which will be retained in the employee's Human Resources file.

12.3 Split Knowledge and Dual Control

To enhance security, symmetric key actions (e.g., key generation or loading) require the collaboration of two custodians authorized by the Internal IT Team. Furthermore, no single custodian may possess or access all components of an asymmetric data encryption key. The separation of public and private encryption keys inherently fulfills the principles of split knowledge and dual control.

12.4 Key Generation

Only strong encryption keys are permitted. Key creation must utilize a random or pseudo-random number generation algorithm. Two custodians, authorized by the Internal IT Team, are required for key generation, with each generating one clear text component for key creation. To prevent unauthorized key substitution, physical and logical access to key generation procedures and mechanisms must be secured.

12.5 Key Distribution

Only custodians authorized by the Internal IT Team are permitted to retrieve key components from secure storage or distribute keys. All such actions must be documented in the Encryption Key Management Log. Before returning to storage, encryption keys must be placed in secure packaging.

12.6 Key Storage

1. All secret and private keys used for encrypting/decrypting cardholder data must be stored encrypted and in the fewest possible locations. Keys must be stored using one or more of the following methods:
2. Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key and stored separately within applicable applications.
3. Within a secure cryptographic device, such as a Hardware Security Module (HSM).
4. As at least two full-length key components or key shares, adhering to an industry-accepted method.
5. Clear-text backups of encryption key components must be stored separately in tamper-evident packaging within a secure location.
6. Key Changes and Destruction
7. A key change involves generating a new key, decrypting current production data, and re-encrypting it with the new key. All data encryption keys must be changed upon reaching the end of their crypto

period or when circumstances necessitate a change to maintain encryption or key integrity. Key changes are required under the following conditions:

8. End of Crypto Period: Keys must be changed once their designated crypto period concludes. Factors influencing the crypto period include algorithm strength, key length, risk of compromise, data sensitivity, and industry best practices.
9. Suspicious Activity: Any activity related to the key process that raises concerns about the existing key's security will trigger a change.
10. Resource Change: Keys must be changed if a resource with key knowledge terminates employment or transitions to a new role no longer requiring access to an encryption process.
11. Technical Requirement: Keys must be changed if their integrity becomes questionable due to technical issues, such as corruption or instability.
12. Encryption keys no longer in service must be disposed of in accordance with the Data Retention and Disposal Policy.

12.7 Transmission Over Untrusted Networks

Confidential and sensitive information must be encrypted when transmitted over networks where interception, modification, or diversion of data is common or easy.

12.8 Email Transmission of Confidential Information

Confidential and sensitive information must never be sent unencrypted via email. Employees with a valid business justification will be issued email encryption software by the Internal IT Team.

12.9 Encryption of Wireless Networks

All wireless networks at Pretense Flip N.V. facilities must be protected through secure data encryption adhering to industry best practices. Wireless encryption keys will be changed every ninety (90) days or whenever an administrator with key knowledge is terminated.

12.10 Non-console and Remote Administrative Access

All non-console (including remote) administrative access must be encrypted using strong cryptography, as outlined in PCI DSS, employing industry-recognized protocols with appropriate key strengths and key management (further detailed in section 11.4 of PCI DSS). Clear-text protocols such as HTTP and Telnet are strictly prohibited for non-console access. Systems must be configured to enforce strong cryptography before any administrator password request.

13 Data Management Policy

13.1 Purpose

This Data Management Policy outlines the Pretense Flip N.V.'s commitment to protecting the personal data of our clients, employees, and stakeholders. It has been developed in strict accordance with applicable data protection laws. This policy governs all systems, individuals, and processes that handle personal data within the Company's information systems.

For the purposes of this policy, "personal data" encompasses information related to:

1. Current, past, and prospective clients
2. Current, past, and prospective employees
3. Other stakeholders (e.g., vendors, partners, job applicants)

13.2 Objectives

Pretense Flip N.V. is dedicated to achieving the following objectives:

1. **Upholding Individual Rights:** To safeguard the rights of individuals concerning the processing of their personal information.
2. **Ensuring Compliance:** To develop, implement, and continuously maintain robust data protection policies, procedures, audit plans, and training programs to ensure full compliance with applicable data protection laws.
3. **Continuous Monitoring:** To diligently monitor every business practice, function, and process within Pretense Flip N.V. for adherence to data protection laws and their core principles.
4. **Lawful Processing:** To process personal data only when a lawful basis for processing, as defined by applicable data protection law, has been clearly established and verified.
5. **Strict Special Category Data Handling:** To process sensitive personal data only in strict compliance with the stringent requirements of applicable data protection law.
6. **Documented Consent:** To accurately record *consent* at the time it is obtained and be prepared to provide verifiable evidence of such consent to the Supervisory Authority upon request.
7. **Competent Workforce:** To ensure that all employees are knowledgeable and competent regarding their data protection obligations. This includes providing in-depth training on data protection principles and regulations, tailored to their specific roles and the Company's operations.
8. **Building Trust:** To foster an environment where individuals feel secure when providing Pretense Flip N.V. with personal information, assured that it will be handled strictly in accordance with their data protection rights.

9. **Proactive Improvement:** To maintain a continuous program of monitoring, review, and improvement in relation to data protection compliance. This includes proactively identifying and addressing any gaps or non-compliance before they escalate into risks, taking necessary mitigating actions.
10. **Staying Informed:** To actively monitor the *local authorities*, updates to stay abreast of changes, notifications, and additional requirements.
11. **Robust Incident Management:** To implement and maintain robust and documented *Complaint Handling and Data Breach controls* for effectively identifying, investigating, reviewing, and reporting any breaches or complaints related to data protection.
12. **Adhering to Retention Policies:** To store and destroy all personal information strictly in accordance with Pretense Flip N.V.'s **data retention policy**.
13. **Employee Awareness of Rights:** To ensure employees are fully aware of their own rights under data protection laws and to provide them with the necessary **Article 13/14 information disclosures** in the form of a dedicated **Privacy Notice**.
14. **Maintaining Processing Records:** To maintain detailed **records of processing activities** in accordance with **Article 30** requirements, where applicable.
15. **Strong Security Posture:** To develop and document appropriate **technical and organizational measures and controls** for personal data security, and to maintain a robust **Information Security program**.
16. **Ongoing Education:** To continuously inform and educate management and employees about the requirements under data protection laws and the potential impact of non-compliance.

13.3 Data Protection Officer (DPO)

Pretense Flip N.V. will appoint a **Data Protection Officer (DPO)**, with the necessary requirements. We will ensure that the assigned individual possesses adequate and expert knowledge of data protection law. The DPO will be assessed as fully capable of assisting Pretense Flip N.V. in monitoring our internal compliance with the regulation and providing support and advice to employees and associated third parties regarding data protection laws and requirements.

13.4 Data Protection Principles

Legal Basis for Processing - Lawfulness of Processing

Personal data is processed lawfully, fairly, and in a transparent manner in relation to the data subject.

At the core of all personal information processing activities undertaken by Pretense Flip N.V. is the assurance and verification that we are complying with ***processing obligations needed***. Prior to carrying out any personal data processing activity, we meticulously identify and establish the legal basis for doing so, verifying these against regulatory requirements to ensure we use the most appropriate legal basis.

The chosen legal basis is clearly documented in our **Privacy Notice** and, where applicable, is provided to the data subject and Supervisory Authority as part of our information disclosure obligations.

Data is only obtained, processed, or stored once we have met all lawfulness of processing requirements.

13.4.1 Conditions for Lawful Processing

Pretense Flip N.V. relies on one or more of the following conditions for the lawful processing of personal data:

1. **Consent:** The data subject has given *consent* to the processing of their personal data for one or more specific purposes.
2. **Contractual Necessity:** Processing is necessary for the *performance of a contract* to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract.
3. **Legal Obligation:** Processing is necessary for *compliance with a legal obligation* to which Pretense Flip N.V. is subject.
4. **Vital Interests:** Processing is necessary in order to *protect the vital interests* of the data subject or of another natural person.
5. **Public Interest/Official Authority:** Processing is necessary for the *performance of a task carried out in the public interest* or in the exercise of official authority vested in Pretense Flip N.V..
6. **Legitimate Interests:** Processing is necessary for the purposes of the *legitimate interests pursued by Pretense Flip N.V. or by a third party*, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, especially where the data subject is a child.

13.4.2 Processing of Special Categories of Personal Data

“Special categories of personal data” are defined in data protection laws as:

1. Data revealing racial or ethnic origin.
2. Political opinions.
3. Religious or philosophical beliefs.
4. Trade union membership.
5. The processing of genetic data.
6. Biometric data for the purpose of uniquely identifying a natural person.
7. Data concerning health.
8. Data concerning a person's sex life or sexual orientation.

Pretense Flip N.V. explicitly states that it does not process special categories of personal data.

13.4.3 Automated Individual Decision Making

Pretense Flip N.V. does not make decisions about persons based solely on fully automated processes.

13.4.4 Limited Purposes

Personal data is collected for specified, explicit, legitimate, and limited purposes, and not further processed in a manner that is incompatible with those purposes.

Personal data may only be processed for the legitimate purpose that was defined before the collection of the data. Subsequent changes to the purpose of the processing are only permissible if the new processing is compatible with the purposes for which the personal data was originally collected.

13.4.5 Data Minimisation

Personal data processing is adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

Pretense Flip N.V. only ever obtains, retains, processes, and shares the data that is **essential** for carrying out its services and/or meeting our legal obligations, and we only retain data for as long as is strictly necessary.

Measures implemented to ensure that only the necessary data is collected include:

1. **Electronic Collection:** Electronic forms (e.g., websites, surveys) are designed to include **only fields that are relevant** to the purpose of collection and subsequent processing. We do not include "optional" fields, as "optional" suggests the data is not necessary.
2. **Physical Collection:** Physical data collection methods (e.g., face-to-face, telephone) are supported by scripts and internal forms where the required data collection is ascertained using predefined fields. Again, only that which is relevant and necessary is collected.
3. **Third-Party Agreements:** We have **Service Level Agreements (SLAs)** and bespoke agreements in place with third-party controllers who send us personal information (whether we act as a controller or processor). These agreements explicitly state that **only relevant and necessary data** is to be provided as it relates to the specific processing activity we are carrying out.
4. **Excess Data Destruction:** We have documented **destruction procedures** in place for instances where a data subject or third party inadvertently provides us with personal information that is surplus to requirement.
5. **Regular Form Review:** Forms, contact pages, and any other documents used to collect personal information are regularly reviewed to ensure they conform with this policy and are obtaining only necessary personal information in relation to the legal basis being relied upon and the purpose of processing.

13.5 Accuracy and Up-to-Date Data

Pretense Flip N.V. keeps personal data accurate and, where necessary, [up-to-date](#). Appropriate measures are adopted to ensure that incorrect or incomplete data is deleted, corrected, supplemented, or updated without delay.

13.5.1.1 Storage Limitation

The Company keeps personal data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

Personal data may only be stored for as long as it is necessary for the purpose for which the data is being processed. This means that personal data must be **deleted or anonymized** as soon as the purpose of its processing has been fulfilled or otherwise lapses, unless specific documentation or retention obligations continue to apply. Those responsible for individual procedures within Pretense Flip N.V. must ensure the implementation of deletion and anonymization routines for their respective processes. Each system handling personal data must have a manual or automated deletion routine. Furthermore, deletion requests

from data subjects, including the removal of personal identifiers, must be technically feasible within our systems.

13.5.2 Integrity and Confidentiality

Personal data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.

Our **"privacy by design"** approach means that we implement company-wide restriction methods for all personal data activities. Restricting access is fundamentally built into Pretense Flip N.V.'s processes, systems, and organizational structure. This ensures that **only those with explicit authorization and/or a relevant business purpose have access to personal information**. Special category data, when hypothetically processed, would be restricted at all levels and accessible only by staff members who are explicitly obliged to perform processing as part of their specific roles (e.g., customer service or development teams, if applicable).

13.6 Data Inventory

Pretense Flip N.V. maintains a comprehensive Data Inventory that describes the types of personal data captured, processed, and stored, along with the terms and conditions under which this data is handled. This inventory details:

- a) The types of personal data Pretense Flip N.V. holds.
- b) The sources from which this data originated.
- c) With whom Pretense Flip N.V. shares this data.
- d) The format(s) in which the data is held.

While using our service, we may ask you to provide us with certain personally identifiable information (hereinafter referred to as "Personal Data"). This may include, but is not limited to:

1. First and last name
2. Residential address
3. Telephone number
4. E-mail address
5. Date of birth
6. Intended use of the account
7. Government identification number
8. Information regarding your source of wealth and source of funds
9. Other subscriber status details

We may use your personal data to contact you with newsletters, marketing, or promotional materials, and other information that may be of interest to you. You may **opt-out** of receiving any, or all, of these communications from us by following the unsubscribe link or the instructions provided in any email we send you.

13.7 Privacy Policy (External)

Pretense Flip N.V. maintains a public-facing **Privacy Policy** (often referred to as our website privacy policy) that includes the most basic yet essential elements:

1. Identification of the site or web application owner (Pretense Flip N.V.).
2. Details of data collected and methods of collection.
3. The **legal basis** for the personal data collection.
4. The **specific purposes** for data collection.
5. The categories of sources from which we collect consumers' personal information.
6. Identification of **third parties who have access to the information**.
7. Details relating to **cross-border/overseas data transfers** and the measures put in place to facilitate these transfers in a safe and compliant way.
8. Clear explanation of **user rights** (e.g., right to access, rectify, erase, or block their data) and how to exercise them.
9. Description of the process for notifying users and visitors of changes or updates to the privacy policy.
10. The effective date of the Privacy Policy.

13.8 Employee Data Processing

13.8.1 Employee Privacy Notice

Pretense Flip N.V. creates and maintains a dedicated Employee Privacy Notice. All employees are required to formally acknowledge this policy. The Employee Privacy Notice clearly explains to an employee how Pretense Flip N.V., as a data controller, processes their personal data.

13.8.2 Data Processing Register for Employees

Pretense Flip N.V.'s HR department maintains a registry for the actions taken with employee data, which must be provided to the regulator upon request in accordance with Article 30.

13.9 Data Retention Policy

For detailed information regarding the retention periods for various types of data, please refer to our dedicated "**Data Ownership and Classification Policy**".

13.10 Data Breach Notification Policy

For comprehensive information on how Pretense Flip N.V. handles data breaches, please refer to our "**Incident Management Policy**".

13.11 Data Subject Consent Form

Consent is one lawful basis for processing personal data, and explicit consent can also legitimize the use of special category data. When relying on consent, we must obtain clear, affirmative permission from the client, typically using a **consent form** that clearly explains the purpose of data processing.

13.12 Data Protection Impact Assessment (DPIA) Register

Pretense Flip N.V. creates and maintains a **DPIA Register** which is used to document our **Data Protection Impact Assessments**. This register helps us identify and mitigate data protection risks for new or high-risk processing activities.

13.13 Data Breach Response and Notification Procedure

For detailed information regarding data breach handling, please refer to our **"Incident Management Policy"**, which covers:

- a) Data Breach Response and Notification Procedure
- b) Data Breach Register
- c) Data Breach Notification Form to the Supervisory Authority

13.14 Third-Party Processors

Pretense Flip N.V. utilizes external third-party processors for certain processing activities. We conduct regular information audits to identify, categorize, and record all personal data that is processed outside of Pretense Flip N.V.. This ensures that the information, processing activity, processor, and legal basis are all recorded, reviewed, and easily accessible.

Our data protection procedures explicitly list our third-party processors and detail the kind of data and processing activities conducted by each.

14 Change Management Policy

14.1 Initiating a Change

Anyone responsible for implementing a system change must submit a [Change Request](#) through our Jira ticketing system. This request should go to the [information or system owners](#) and clearly outline the [minimum data](#) ⁷⁰ r [electronic capture](#). This Change Request typically takes the form of a [ticket](#), which will then be reviewed and [approved by the system owner](#).

Each ticket must include:

1. **Affected Resources:** A list of all resources impacted by the change.
2. **Business Analysis & Functionality:** A description of the business reason for the change and any resulting functional modifications.
3. **Back-Out Procedures:** A detailed plan to revert the environment to its original configuration if the change doesn't go as intended.
4. **Test Plan:** A set of planned tests to verify the change's success. This plan must ensure the change doesn't negatively impact other system components or create security vulnerabilities. Each change might require a specific test plan.

14.2 Testing Requirements

Before any change is introduced into our production network or systems, it must be thoroughly tested on a QA or test network that's isolated from the production environment. We must rigorously follow the documented test plan to prevent any adverse effects on the network, systems, or applications. Additionally, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and all documentation needs to be updated accordingly.

14.3 Change Reporting

A [monthly report](#) detailing the progress of our change process will be issued to the management board. If we're using an agile methodology, this report can take the form of a real-time information radiator.

The report must, at a minimum, include:

1. **New Issues:**
 - a) Business features and changes
 - b) Technical issues
 - c) New bugs found
2. **Issues in Progress**
3. **Solved Issues**
4. **Currently Blocked Issues** (along with the reasons for blockage)

⁷⁰ISO 27001 A.12.1.2

15 Incident Management Policy⁷¹

15.1 Purpose

The purpose of this policy is to define the process for effectively managing information security incidents within Pretense Flip N.V. This includes identifying, reporting, assessing, responding to, resolving, and learning from incidents, with the goal of minimizing disruption to business operations and protecting our information assets.

15.2 Scope

This policy applies to all employees, contractors, and third parties who interact with or manage information systems and data belonging to Pretense Flip N.V.. It covers all information assets, systems, and services, whether internal or external.

15.3 Policy Statements

15.3.1 Incident Identification and Reporting

1. All personnel must be vigilant and immediately report any suspected information security incidents or events.⁷²
2. Incidents should be reported on **Jira** Ticketing systems, and an email to itsupport@mtmgroup.io as soon as they are detected.
3. Reports should include as much detail as possible, such as:
 - a) What happened (or what is suspected).
 - b) When it happened.
 - c) Where it happened (affected system, application, or data).
 - d) Any visible symptoms or error messages.
 - e) Who discovered it.

15.3.2 Incident Assessment and Triage⁷³

1. Upon receiving an incident report, the IRT will promptly assess the reported event to determine if it constitutes an actual information security incident.
2. Incidents will be categorized and prioritized based on their potential impact on business operations, data sensitivity, and the urgency of response.
3. Initial steps to contain the incident and prevent further damage will be initiated immediately.

⁷¹ISO 27001 A.16

⁷²ISO 27001 A.16.1

⁷³ISO 27001 A.16.1.6

15.3.3 Incident Response and Resolution⁷⁴

1. The IRT will execute a response plan tailored to the specific incident. This may involve:
 - a) **Containment:** Limiting the spread and impact of the incident.
 - b) **Eradication:** Removing the cause of the incident (e.g., malware, unauthorized access).
 - c) **Recovery:** Restoring affected systems and data to normal, secure operation.
 - d) **Investigation:** Gathering evidence for analysis and understanding the root cause.
2. All actions taken during incident response must be thoroughly documented.

15.4 Communication

- The IRT is responsible for communicating incident status to relevant internal stakeholders (e.g., management, affected departments).
- External communication (e.g., to law enforcement, regulators, affected customers) will only be conducted by authorized personnel and in accordance with legal and regulatory requirements.

15.4.1 Post-Incident Review

1. For all significant incidents, a post-incident review (lessons learned) will be conducted by the IRT and relevant stakeholders.
2. The review will identify:
 - a) What went well and what could be improved during the response.
 - b) The root cause(s) of the incident.
 - c) Recommendations for improving security controls, policies, or procedures to prevent recurrence.
2. Actionable recommendations will be documented and assigned to responsible parties.

15.4.2 Training and Awareness

1. All employees will receive regular training on how to identify and report information security incidents.
2. The IRT will receive specialized training to ensure they have the necessary skills and knowledge to effectively respond to incidents.

15.5 Responsibilities

1. **Management:** Provides resources and support for incident management and ensures policy compliance.
2. **Information Security Officer (ISO) / IT Manager:** Oversees the incident management process and leads the IRT.
3. **Incident Response Team (IRT):** Responsible for executing incident response procedures.
4. **All Employees:** Responsible for reporting suspected incidents and cooperating with the IRT during an investigation.

15.6 Policy Review

This policy will be reviewed at least annually, or more frequently if there are significant changes to our information systems, threat landscape, or regulatory requirements.

16 Information Security Risk Management Policy

16.1 Introduction & Purpose

This policy sets out Pretense Flip N.V.'s approach to managing information security risks. It establishes the framework, controls, processes, and procedures we use to identify, assess, and address risks to all Pretense Flip N.V. assets—whether owned, operated, or utilized by us. This includes all company information and technology, and applies to every individual who accesses it, including external partners who process data on our behalf.

We define **risk** as the potential for an event or entity to threaten our operations, considering both the **likelihood** of that event occurring and the **adverse effects** it would have. While we actively reduce risks, we acknowledge that **zero risk is unachievable**; a certain level of risk must always be accepted as part of doing business.

Cybersecurity risks can stem from external threats or internal actions. These risks encompass any operational threat to our information and technology assets that could impact their **availability, integrity, or confidentiality**. This includes physical or technical vulnerabilities in our networks, computers, programs, and data. Our focus extends to all information flowing through or supported by our digital infrastructure, information systems, and industrial control systems, covering areas like information security, supply chain assurance, and hardware and software integrity. The process outlined in this policy helps us understand and manage these risks, which we model as the likelihood of adverse events multiplied by their potential impact.

16.2 Our Objectives⁷⁵

This policy and its supporting procedures provide a consistent, organized, and common framework for information security risk management across Pretense Flip N.V.. This ensures we understand and manage risks reliably and uniformly.

Our key objectives for information risk management are to:

1. **Identify & Assess:** Proactively find and evaluate all information risks.
2. **Manage & Treat:** Handle all identified risks in line with Pretense Flip N.V.'s acceptable risk levels.
3. **Implement Controls:** Establish and maintain appropriate security measures for all our information assets.
4. **Align with Best Practices:** Ensure our approach matches leading industry standards and practices in information security.

16.3 Risk Governance⁷⁶

Pretense Flip N.V.'s risk framework is overseen by our **Risk Review Group**, which includes:

1. The Chief Executive Officer (CEO)
2. The Chief Technology Officer (CTO)
3. Chief Security Officer (CSO) & Head of Legal

This group supports the Board of Directors in risk management by holding regular reviews. Additionally, both our internal and external IT departments have their own Risk Managers who report directly to the Pretense Flip N.V. Risk Review Group.

16.4 The Security Risk Register⁷⁷

We document all information security risk assessment results and actions in a dedicated **Information Security Risk Register**. This ensures clear visibility of all risks related to information and cybersecurity.

Where appropriate, we will communicate relevant risks to departments and external service providers. They will then log, track, and escalate these risks within their own local risk registers.

For each risk, the register will detail a **risk treatment decision** falling into one of these categories:

1. **Tolerate (Accept):** When the risk is already within our acceptable limits, and further action isn't practical or necessary.
2. **Treat (Mitigate):** When the risk exceeds our acceptable limits and taking action is practical. This also applies if a simple, cost-effective treatment exists for a risk, even if it's already low.
3. **Transfer (Share):** When we can't reduce the risk to acceptable levels with our own efforts, but we can cost-effectively shift it to a third party (e.g., through insurance).
4. **Terminate (Avoid):** When the risk cannot be brought to an acceptable level, and there's no cost-effective way to transfer it, leading us to stop the activity causing the risk.

16.5 Risk Appetite⁷⁸

Our **risk appetite** reflects how much risk Pretense Flip N.V. is willing to accept concerning potential threats and vulnerabilities.

- a) For **mission-critical or high-importance services** like card payments or bank transfers, our Internal IT Team maintains a **low-risk appetite**. This means we take very few chances with these areas.
- b) For other services where we need to **experiment, innovate, or use cutting-edge technologies**, Pretense Flip N.V. has a **moderate risk appetite**. We're open to more risk here, provided it's properly managed.

Any decision to tolerate or transfer a risk must be thoroughly documented by the Risk Review Group, justified, and formally approved by an appropriate staff member. Treatment plans also require approval from relevant personnel.

16.6 Policy Development & Updates

We continuously measure the effectiveness of this policy and our information security risk framework to ensure they remain fit for purpose, consistent, and sustainable. This involves an **annual review** to assess the policy's effectiveness against its goals. We will update the policy to reflect any approved changes to our risk management framework.

We'll implement this policy and framework through ongoing collaboration with all stakeholders, departments, and third parties.

⁷⁷PCI DSS 8.1⁷⁸PCI DSS 8.2

16.7 Risk Communication & Review

Risk management is an **ongoing and vital part** of our cybersecurity efforts. Our process doesn't end once risks are addressed. We must continuously analyse how successful our solutions were and make adjustments as needed.

A key part of this is **risk communication**. This involves keeping clear records of how we're tackling risks and ensuring anyone who might be affected is kept informed.

17 Internet, Email, and Digital Asset Usage Policy

17.1 Purpose and Scope

This policy outlines the acceptable use of Pretense Flip N.V.'s internet, email, and digital resources, establishing clear guidelines for all employees. Our aim in providing access to these tools is to facilitate essential business operations while safeguarding company assets, maintaining a secure digital environment, and ensuring compliance with legal and ethical standards.

17.2 Ownership and Monitoring

All computers, network components, software, and data stored on company devices, media, or networks are the sole property of Pretense Flip N.V.. This includes, but is not limited to, all internet Browse history, email communications, and files created or stored using company resources.

Pretense Flip N.V. reserves the right to monitor, inspect, and audit all digital activity on its networks and devices, including internet usage, email content, and system logs. This monitoring is conducted to ensure compliance with this policy, protect company interests, and maintain the security and integrity of our systems. Employees should have no expectation of privacy when using company-owned resources.

17.3 Internet Usage Policy⁷⁹

All employees requiring internet access must do so exclusively through Pretense Flip N.V.'s approved software and network gateways. The following activities are strictly prohibited:

1. Accessing, downloading, or distributing illicit, inappropriate, or offensive content, including but not limited to, pornography, hate speech, or content promoting illegal activities.
2. Visiting websites associated with hacking, malware distribution, or other dubious or malicious purposes.
3. Downloading, installing, or executing any software, applications, or files from the internet without explicit, prior authorization from the IT department.
4. Engaging in any activity that could compromise the security, integrity, or performance of Pretense Flip N.V.'s networks, systems, or data.
5. Using company internet access for extensive personal use that interferes with job performance, consumes excessive bandwidth, or violates any other aspect of this policy.

Please be aware that web browsers maintain a record of all websites visited, creating a digital footprint that is auditable by the company.

17.4 Exceptions for Security Personnel

Pretense Flip N.V. security technicians may require access to certain sites of a dubious nature for monitoring security vulnerabilities, conducting threat analysis, or performing other security-related exercises. Such access must be pre-approved, carried out from isolated systems that do not contain sensitive data, and conducted with the utmost caution and adherence to established security protocols.

⁷⁹ISO 27001 A.15.10 – A 5.15- PCI DSS 12.6

17.5 Email Usage Policy⁷⁹

Pretense Flip N.V.'s email system is provided for business-related communications. All emails sent and received via company accounts are considered company property and are subject to monitoring and retention. Employees must adhere to the following guidelines:

1. **Professional Conduct:** All email communications must be professional, respectful, and appropriate for a business environment. Harassing, discriminatory, threatening, or offensive content is strictly prohibited.
2. **Confidentiality:** Do not use company email to transmit or store sensitive, confidential, or proprietary company information to unauthorized individuals or external entities without proper authorization and security measures.
3. **Personal Use:** Limited personal use of company email is permitted during non-working hours or breaks, provided it does not interfere with job duties, consume excessive resources, or violate any other aspect of this policy.
4. **Attachments:** Exercise extreme caution when opening email attachments, especially from unknown senders. Report any suspicious emails immediately to the IT department. Do not open attachments that you are not expecting or that seem unusual.
5. **Phishing and Spam:** Do not respond to suspicious emails (phishing attempts) or forward chain letters, spam, or unsolicited commercial emails.
6. **Legal Compliance:** Do not use company email for any activities that are illegal or violate any applicable laws or regulations.

17.6 Non-Business Browse

Limited non-business internet Browse is permitted during designated breaks (e.g., lunch breaks, coffee breaks) provided it does not:

1. Interfere with your job responsibilities or the productivity of others.
2. Consume excessive network bandwidth or system resources.
3. Violate any of the usage restrictions outlined in the "Internet Usage Policy" section above.

17.7 Compliance and Enforcement⁷⁹

All employees are required to understand and comply with this policy. Any violations will result in disciplinary action, which may include, but is not limited to, verbal warnings, written warnings, suspension, and immediate termination of employment. Legal action may also be pursued if warranted.

Employees who become aware of any violations of this policy are obligated to report them immediately to the Information Security Officer. The identity of any employee reporting a violation will be kept strictly confidential.

18 Pretense Flip N.V. Password Security Policy⁸¹

18.1 Purpose

At Pretense Flip N.V., strong passwords are the first line of defence for our digital assets. This policy ensures that all users create and maintain secure passwords, safeguarding our systems and the sensitive information they hold. By adhering to these guidelines, we protect company data, maintain operational continuity, and prevent unauthorized access.

18.1.1 Who This Policy Applies To

This policy applies to everyone who accesses Pretense Flip N.V.'s systems, including all employees, contractors, consultants, and any third parties granted access to our IT infrastructure. If you have a password for an Pretense Flip N.V. system, this policy is for you.

18.2 Your Password, Your Responsibility

Each user is assigned a unique password for system access. **Your password is yours alone**, and you are solely responsible for its security and proper use. Under no circumstances should you share your password with anyone, including colleagues, managers, or IT personnel.

You'll be asked to acknowledge or agree to a statement confirming your understanding of the importance of keeping your authentication information confidential. Your adherence to this policy is a critical part of your responsibility to Pretense Flip N.V..

18.3 Crafting a Strong Password⁸²

A strong password is your primary defence against unauthorized access. All passwords must meet the following composition requirements:

1. **Minimum Length:**
 - a) **10 characters** for standard users.
 - b) **15 characters** for "superuser" accounts (e.g., administrators, users with access to sensitive data like payroll).
2. **Complexity:** Your password must include characters from at least **three** of the following categories:
 - a) Uppercase letters (A, B, C...)
 - b) Lowercase letters (a, b, c...)
 - c) Numbers (0, 1, 2...)
 - d) Special characters (!, @, #, \$, %, ^, &...)

• ⁸¹ISO 27001 A 9.2.4
⁸²PCI DSS 8.2.3

3. **Prohibited Patterns:** To prevent easy guessing, avoid using:
-

- a) Dictionary words (in any language).
- b) Personal information (e.g., names of family members, pets, or your telephone number).
- c) Vehicle registration numbers or other easily discoverable IDs.
- d) Your user ID or any part of it.
- e) Simple sequences or repetitions (e.g., "123456", "aaaaaa", "qwerty").

18.4 Maintaining Password Security

Beyond creation, the ongoing maintenance of your password is vital:

1. **Temporary Passwords:** If you receive a temporary password, you **must change it immediately** upon your first login. Temporary passwords will be issued securely, avoiding external email, unsecured email, or chat platforms.
2. **Regular Changes:**
 - a) For **high-risk systems** (e.g., those containing sensitive customer data or critical infrastructure), passwords must be changed at least every **120 days**.
 - b) For **lower-risk systems**, passwords should be updated every **180 to 360 days**.
 - c) If you're unsure about a system's risk level, consult the system/data owner or the Internal IT Team.
3. **No Writing Down:** **Never write down your password** in an unsecured location. This includes sticky notes, notebooks, or unencrypted digital files.
4. **No Sharing:** Under no circumstances should passwords be shared via email, messaging platforms (regardless of their claimed security), or any other unsecure method.
5. **Identity Verification:** When requesting a password reset or new authentication information, be prepared to verify your identity through established procedures to protect your account.

18.5 Critical System Passwords

The Internal IT Team manages crucial passwords that control core Pretense Flip N.V. systems (e.g., firewalls, applications, backup utilities, email and web servers). The security of these passwords is paramount to our business continuity.

Owners of these critical passwords **must** document them on a memo, seal them in a signed and taped envelope, and store them in a secure safe under management control. These envelopes are only to be opened in emergencies when no other access method is available. A history of these passwords will also be maintained for system restoration purposes.

18.6 Credentials Register

Pretense Flip N.V. maintains a centralized Credentials Register that lists all IT assets, the individuals with access to each, and their respective access levels. This register is regularly updated by IT asset owners whenever changes occur, ensuring clear oversight of who has access to what.

18.7 Password Monitoring and Enforcement

Pretense Flip N.V. may periodically use common password cracking tools to test the strength of passwords on our systems. If a weak password is identified, the affected employee will be privately notified, required to change it immediately, and advised on creating a stronger one.

Wherever possible, Pretense Flip N.V.'s IT systems are configured to automatically enforce the password policies outlined in this document. This proactive approach significantly reduces the risk of insecure passwords being used. We prioritize the development or acquisition of software that supports and enforces these security standards.

19 Anti-Virus policy

19.1 Purpose

The purpose of this policy is to:

1. Minimize the risk of malware infections, including viruses, worms, Trojans, ransomware, spyware, adware, and other forms of malicious code.
2. Protect all systems, networks, and data, especially those involved in the storage, processing, or transmission of cardholder data.
3. Ensure the timely detection, containment, and eradication of malware threats.
4. Comply with regulatory requirements, including PCI DSS Requirement 5 and ISO 27001 Annex A 8.7.
5. Establish clear responsibilities for malware protection.

19.2 Scope

This policy applies to:

1. All employees, contractors, temporary staff, and third parties who access or use Pretense Flip N.V. information systems and networks.
2. All information systems, including but not limited to:
 - a) Servers (physical and virtual)
 - b) Workstations (desktops, laptops)
 - c) Mobile devices (if permitted to access organizational data/systems)
 - d) Network devices (where applicable for anti-malware scanning)
 - e) Cloud-based services and infrastructure (where anti-malware controls are applicable)
 - f) Removable media (USB drives, external hard drives, etc.)
 - g) Email systems and web Browse
 - h) Any system component that could be affected by malicious software.

19.3 Policy Statements

19.4 Anti-Malware Solution Deployment⁸³

1. Approved anti-malware software must be deployed on all systems commonly affected by malicious software. This includes, but is not limited to, all workstations, servers, and other systems connected to the Cardholder Data Environment (CDE) or processing sensitive information.

● ⁸³ISO 27001 A 8.7 PCI DSS Requirement 5

2. The anti-malware solution must be centrally managed and configured to provide real-time, on-access scanning and protection.
3. The anti-malware solution must be from a reputable vendor and provide effective detection and prevention capabilities.
4. Solutions must be actively running and configured such that they cannot be disabled or altered by users unless specifically authorized by the [IT Department / Information Security Team] for a limited time period.

19.5 Anti-Malware Updates and Patching

1. Anti-malware definitions/signatures must be automatically updated at least daily, or more frequently as recommended by the vendor and justified by risk.
2. The anti-malware software engine and associated components must be regularly updated to the latest stable versions, following the organization's patch management policy.
3. Mechanisms must be in place to verify that updates are successfully applied across all deployed solutions.

19.6 Regular Scans⁸⁴

1. All systems covered by this policy must undergo regular, scheduled anti-malware scans.
2. Full system scans must be performed at least [daily/weekly/monthly – *adjust based on risk and system criticality*].
3. All files accessed, downloaded, or introduced via removable media or network transfers must be scanned in real-time by the anti-malware solution.
4. Email attachments and instant messaging downloads must be scanned prior to opening.
5. Web content accessed by users must be scanned and filtered for malicious content.

19.7 Malware Detection and Response⁸⁵

1. Systems must be configured to generate alerts upon malware detection or suspicious activity.
2. All malware alerts and incidents must be logged, monitored, and promptly investigated by the [Information Security Team / IT Department].
3. An Incident Response Plan (refer to the [Your Organization Name] Information Security Incident Response Policy) must be in place and regularly tested to address malware breaches effectively, including containment, eradication, recovery, and post-incident review.
4. Infected systems must be isolated immediately to prevent further spread of malware.
5. Remediation procedures must be followed to remove the malware and restore the system to a secure state. This may include system re-imaging if necessary.

⁸⁴ISO 27001 A 8.2.1 PCI DSS 5.3

⁸⁵ISO 27001 A 5.21 PCI DSS 12.2

19.8 Removable Media and External Devices

1. The use of unauthorized removable media is prohibited.
2. All authorized removable media must be scanned for malware before being connected to any system within [Your Organization Name]'s environment.
3. Procedures for handling and scanning external devices (e.g., guest laptops) must be defined and enforced if they are permitted to connect to the network.

19.9 Email and Web Security

1. Email systems must employ anti-malware and anti-spam solutions to filter and scan incoming and outgoing emails for malicious content.
2. Web Browse must be protected by web filtering solutions that block access to known malicious websites and prevent the download of unauthorized or malicious files.

19.10 User Awareness and Training⁸⁵

1. All personnel must receive regular information security awareness training, which includes specific modules on malware threats, phishing, social engineering, and safe computing practices.
2. Users must be trained on how to identify and report suspicious activities or potential malware infections.
3. Users are prohibited from disabling or circumventing anti-malware controls.

19.11 Review and Monitoring⁸⁶

1. Anti-malware logs must be centrally collected, securely stored, and regularly reviewed for suspicious activity.
2. The effectiveness of the anti-malware solution and this policy must be reviewed at least annually, or in response to significant changes in the threat landscape or organizational infrastructure.
3. Any exceptions to this policy must be formally documented, justified by a risk assessment, approved by the [Information Security Manager / Management], and reviewed periodically.

⁸⁵ISO 27001 A 8.7-PCI DSS 12.6

⁸⁶ISO 27001 A 7.9-PCI DSS A 5.2

20 Secure Mobile Computing

20.1 Purpose and Scope

This policy outlines the requirements for the secure use and handling of all company-owned and managed portable computing devices, including laptops, tablets, smartphones, and other mobile devices capable of storing or accessing organizational data. Given their inherent portability, these devices are highly susceptible to physical loss, damage, or unauthorized access, especially when used outside the organization's-controlled environments. This policy aims to minimize these risks, safeguard sensitive information (including cardholder data and personal data), and maintain business continuity.

This policy applies to all personnel (employees, contractors, temporary staff, etc.) who are issued or use company-provided portable devices.

20.2 Responsibilities and Accountabilities

All personnel using company-provided portable computing devices are accountable for adhering to the following directives and contributing to the overall security posture of the organization. Violations of this policy may result in disciplinary action up to and including termination of employment, and where applicable, legal action.

20.3 Policy Directives

20.3.1 Device Physical Security & Access Control⁸⁷

Secure Device Access: All portable devices must be configured with a strong authentication mechanism (e.g., password, PIN, fingerprint, pattern lock) to unlock the screen. Devices must be immediately locked or logged off when unattended, even for brief periods.

Protection Against Loss/Theft:

1. Devices shall never be left unattended in public or unsecured areas.
2. When not in active use, devices must be stored in secure locations (e.g., locked drawers, cabinets, or carrying cases).
3. Devices left in vehicles must be secured out of sight (e.g., in a locked boot) and only when absolutely necessary for short durations. Transporting devices with the individual is always preferred.⁸⁸
4. **Physical Protection:** Devices must be transported and stored in appropriate protective cases to minimize the risk of accidental damage.⁸⁸

20.3.2 Data Protection and Encryption⁸⁹

1. **Mandatory Encryption:** All company-issued laptops and portable devices capable of storing company data, especially sensitive information (including cardholder data and personal data), must utilize approved full-disk encryption or equivalent data-at-rest encryption technologies. Encryption of data on removable media (e.g., USB drives) used for company data is also required whenever feasible.

⁸⁷ISO 27001 A 5.15,18-PCI DSS 8.1,8.2⁸⁸ISO 27001 A 7.7 & A.7.9-PCI DSS 9.4-⁸⁹ISO 27001 A 8.2.1-A8.2.3-PCI DSS3.4,4.1

2. Data Backup: Users are responsible for regularly backing up critical company data stored on their portable devices to approved company network storage solutions. In instances where network access is not feasible, data may be backed up to encrypted removable media (e.g., USB drives, external hard drives) following established procedures. Backups should be performed at least weekly.⁹⁰
3. Data Minimization: Personnel should strive to store only the necessary company data, particularly personal data or cardholder data, on portable devices to minimize exposure in case of loss or theft.⁹¹

20.3.3 Responsible Device Usage

1. Exclusive Business Use: Company-owned devices are provided for business purposes and must not be shared with unauthorized third parties, including family members or friends.⁹²
2. Software Installation: Only authorized and approved software may be installed on company-owned devices. Unauthorized software installations are prohibited.⁹³
3. Network Connectivity: Exercise caution when connecting to untrusted networks (e.g., public Wi-Fi). Always use approved Virtual Private Network (VPN) connections when accessing company resources from external networks.⁹³
4. Malware Protection: All portable devices must have approved anti-malware software actively running with up-to-date definitions. Users must not disable or bypass these security controls.⁹³

20.3.4 Incident Reporting

1. Immediate Reporting of Loss/Theft: The loss or theft of any company-owned portable device must be reported immediately to the direct supervisor and the Internal IT Team. Prompt reporting is critical to enable remote wiping, password changes, and activation of incident response procedures.⁹⁴
2. Reporting Unauthorized Access/Compromise: Any suspected unauthorized access to a device or compromise of data on a device must also be reported immediately to the Internal IT Team.⁹⁴

⁹⁰ISO 27001 A 8.2.3,A 17.1.2-PCI DSS 10.7

⁹²ISO 27001 A 5.10, A 5.18-PCI DSS 12.3

⁹³ISO 27001 A 8.7,PCIDSS 6.2

⁹⁴ISO 27001 A 16.1.1-PCI DSS 12.10

21 Internet & Software Usage Policy

21.1 Purpose

This policy establishes guidelines for the responsible and secure use of company internet access and software, including cloud-based applications. Its purpose is to safeguard organizational information, ensure compliance with legal and regulatory obligations (e.g., PCI DSS for cardholder data, Data Protection Law / Legislation for personal data), prevent malicious activities, and maintain operational efficiency.

21.2 Scope

This policy applies to all personnel (employees, contractors, temporary staff) accessing company networks, systems, or data via the internet, and using any company-provided or approved software, regardless of device ownership or location.

21.3 Policy Directives

21.3.1 Internet Usage

1. **Business Use Primary:** Internet access is primarily for business purposes. Limited, reasonable personal use is permitted, provided it does not interfere with job duties, consume excessive bandwidth, or violate any other company policies.
2. **Prohibited Activities:** Accessing, downloading, or transmitting illegal, offensive, or inappropriate content (e.g., pornography, hate speech, illegal streaming, gambling) is strictly prohibited.
3. **Security Awareness:** Users must exercise caution regarding suspicious links, unsolicited emails (phishing), and unverified downloads to prevent malware infections or security compromises.
4. **Sensitive Data Transmission:** Sensitive company data, including cardholder data or personal data, must only be transmitted over approved, secure (e.g., encrypted) channels.
5. **Monitoring:** All internet usage on company networks and devices is subject to monitoring for security, compliance, and policy enforcement purposes.⁹⁵

21.3.2 Software Usage

1. **Authorized Software Only:** Only company-approved and licensed software may be installed and used on company devices and systems. Unauthorized software installation is prohibited.
2. **Software Updates:** Users must ensure that operating systems and applications on company devices are kept up to date with the latest security patches and updates. Automatic updates should be enabled where possible.
3. **Malware Protection:** All systems must run active and up-to-date anti-malware software, which must not be disabled. Users are responsible for reporting any suspected malware incidents.
4. **Data Handling:** Software must be used in a manner consistent with data classification guidelines, especially when handling sensitive information, cardholder data, or personal data. Data stored in cloud services must adhere to organizational data residency and security requirements.⁹⁶

⁹⁵ISO 27001 A 5.10, A 13.2-PCI DSS 12.3,12.6

⁹⁶ISO 27001 A 8.7,A 5.10,A 8.2-PCIDSS 5.1,5.2,5.3,6.2

21.4 Incident Reporting

Any suspected or actual security incidents related to internet use or unauthorized software, including malware infections or data breaches, must be immediately reported to the Internal IT Team.⁹⁷

⁹⁷ISO 27001 A 5.10, A 16.1-PCI DSS 12.10,12.6

22 Security Testing and Vulnerability Management Policy

22.1 Purpose and Scope

This policy defines the requirements for establishing, implementing, and maintaining robust security testing, vulnerability identification, and remediation processes across all information systems and network devices within Pretense Flip N.V., regardless of whether they are managed internally or by third parties. The objective is to proactively identify, assess, and address security weaknesses to protect the confidentiality, integrity, and availability of organizational information, including sensitive data such as Cardholder Data (CD) and Personal Data (PD), and to ensure continuous compliance with relevant standards and regulations.

Exemptions from this policy require prior written approval from the Head of Engineering (HOE) or Chief Information Security Officer (CISO), justified by a documented risk assessment.

22.2 Secure System Design and Deployment⁹⁸

All information systems, including servers and network devices, must be designed, built, and deployed with security as a foundational principle. Where technically feasible and beneficial for security segmentation, systems should be designated for a single primary function (e.g., separating web, database, and DNS services onto distinct servers or virtual instances). This approach supports the principle of least privilege and reduces the attack surface.

22.3 Change Detection and Integrity Monitoring⁹⁹

Pretense Flip N.V. shall implement and maintain change-detection solutions, such as File Integrity Monitoring (FIM) software, on all critical systems. Critical systems are defined as those storing, processing, or transmitting sensitive data (including CD and PD), or those that significantly impact the security of such data.

The change-detection solution must monitor all relevant user and system activity that could impact file integrity on critical systems.

Reporting and alerting mechanisms shall be enabled to automatically notify key personnel when unauthorized or suspicious changes occur to critical files (e.g., system executables, application executables, configuration files, content files, log, and audit files).

Critical file comparisons shall be performed by the solution at least weekly.

Alerts generated by the change-detection solution must be continuously reviewed by the Internal IT Team to determine if incident response actions are necessary.

Any unauthorized changes to systems containing confidential or sensitive information must trigger immediate notification to the Internal IT Team and initiation of defined incident response procedures.

⁹⁸ISO 27001 A 5.10, A 8.1-PCI DSS 2.2,16.3⁹⁹927001 A 8.7, A 13.2.1,A 16.1-PCI DSS 10.5.5, 11.5

22.4 Vulnerability Identification and Assessment¹⁰⁰

The Internal IT Team is responsible for a systematic process of identifying, assessing, and communicating information security vulnerabilities applicable to Pretense Flip N.V.'s computing systems and network infrastructure.

1. Vulnerability Awareness: The Internal IT Team shall proactively stay informed about emerging information security issues and vulnerabilities relevant to Pretense Flip N.V.'s technology stack.
2. Vulnerability Ranking: Discovered security vulnerabilities will be assigned a risk ranking (e.g., "Critical," "High," "Medium," "Low") based on their potential impact and likelihood of exploitation, informing prioritization for remediation.

Vulnerability Scanning:

1. Internal and external network vulnerability scans shall be conducted at least quarterly.
2. Scans must also be performed after any significant change to the networked environment (e.g., new system component installations, changes in network topology, firewall rule modifications, major product upgrades, etc.).
3. These scans must include the identification of unauthorized wireless devices connected to the network.
4. Internal vulnerability scans shall be performed by qualified internal personnel.
5. External vulnerability scans targeting the perimeter of the Cardholder Data Environment (CDE) must be performed at least quarterly by an Approved Scanning Vendor (ASV) qualified by the Payment Card Industry.
6. Penetration Testing:
7. Internal and external penetration tests, covering both application and network layers, shall be performed annually or after any significant change in the network or applications.
8. Pretense Flip N.V.'s penetration tests shall adhere to industry-accepted methodologies and comprehensively cover the entire CDE perimeter and critical systems.
9. Segmentation controls and any mechanisms used to isolate the CDE from other networks must be rigorously tested to confirm their effectiveness. A penetration test of segmentation controls is mandatory whenever changes are made to these controls/methods, otherwise it must be performed annually.
10. Prioritized consideration shall be given to vulnerabilities and threats experienced by the organization or the industry within the preceding 12 months during planning of penetration tests.

Reporting and Remediation:

1. All potential vulnerabilities identified through vulnerability scans and penetration tests shall be formally communicated to relevant personnel within Pretense Flip N.V. for assessment and remediation planning.
2. All high-risk vulnerabilities must be remediated promptly in accordance with Pretense Flip N.V.'s defined risk acceptance and remediation policies.
3. Follow-up scans or re-tests must be performed to verify that all identified "high-risk" vulnerabilities have been effectively resolved.
4. Annual Risk Assessment: The Chief Technology Officer shall coordinate an annual formal risk assessment process that systematically identifies new and existing threats and vulnerabilities,

ensuring that Pretense Flip N.V.'s information assets and personal data are adequately protected against evolving risks.

¹⁰⁰ISO 27001 A 6.1.2, A 8.7, A 9.4.1-PCI DSS 6.1,11.2,11.3,12.2

22.5 Security Patch Management¹⁰¹

All security patches, hotfixes, and service packs identified by the Internal IT Team or system administrators as applicable to Pretense Flip N.V.'s systems must be assessed and applied within thirty (30) days of vendor release, unless a documented risk assessment justifies a different timeline.

The application of security patches shall adhere to Pretense Flip N.V.'s established change management process, including testing to prevent adverse impacts on system functionality or security.

¹⁰¹ISO 27001 A 6.1.2, A 8.7, A 14.2.2-PCI DSS 6.2

23 Secure Access & Critical Systems Policy

23.1 Purpose & Scope

This policy governs the secure access to and usage of Pretense Flip N.V.'s critical systems and technologies, which, due to their nature, pose a heightened risk to information assets, including Cardholder Data (CD) and Personal Data (PD). It applies to all personnel (employees, contractors, third parties) utilizing such technologies within Pretense Flip N.V.'s environment. This policy supports the protection of confidentiality, integrity, and availability, ensuring compliance with relevant standards and regulations.

Exemptions require prior written approval from the Chief Technology Officer (CTO) & Chief Information Security Officer (CISO) and a documented risk assessment. Currently identified critical technologies include, but are not limited to, remote access, wireless networks, portable devices (laptops, tablets, mobile phones), and Internet access within Pretense Flip N.V.'s computing environment. This policy will be updated as new critical technologies are identified.

23.2 Controlled Access & Approval¹⁰²

Access to and deployment of critical technologies must be explicitly approved by the Internal IT Team. This approval is based on job function or individual need and must be formally documented (e.g., on an "Authorisation Request Form"). Specific critical access requiring this approval includes VPN and wireless network access.

23.3 Authentication Requirements¹⁰²⁻¹⁰³

All access to critical technologies and systems must be securely authenticated.

1. **Integration:** Authentication mechanisms should, where feasible, integrate with Pretense Flip N.V.'s central identity management systems.
2. **Minimum Authentication:** Devices must be authenticated using at least a strong username and password, or another approved authentication factor (e.g., hardware token). Password policies (complexity, change intervals) must adhere to existing Pretense Flip N.V. security standards.
3. **Multi-Factor Authentication (MFA):** All remote access to Pretense Flip N.V.'s network (for general users, administrators, and vendors) and all non-console/remote administrative access to the Cardholder Data Environment (CDE) must utilize strong multi-factor authentication approved by the Internal IT Team.

23.4 Device Inventory & Identification¹⁰⁴

Pretense Flip N.V. and its essential third-party partners must maintain a current and accurate inventory of all approved devices utilized for critical technology access. This inventory must include, at a minimum, the device's serial number, type, description/model, condition, year of fabrication/purchase, owner, employee details, and function.

Users granted access to critical technologies (e.g., wireless network users, personnel with sensitive system access, vendors with access) must be formally documented in a "Critical Technologies Devices Log."

¹⁰²ISO 27001 A 5.15,A 5.18-PCI DSS 12.3

¹⁰³PCI DSS 8.2,8.3

¹⁰⁴ISO 27001 A 8.1.1-PCI DSS 2.4,2.5

24 Physical Security and Access Control Policy

24.1 Purpose & Scope

This policy establishes the requirements for safeguarding Pretense Flip N.V.'s physical premises, information processing facilities, and sensitive areas from unauthorized access, damage, and environmental threats. It outlines controls to ensure the physical security of all assets, including sensitive data (Cardholder Data, Personal Data), and to maintain compliance with relevant standards and regulations. This policy applies to all Pretense Flip N.V. facilities, personnel, visitors, and third-party personnel.

24.2 Access Control for Visitors & Personnel¹⁰⁵

24.2.1 Visitor Management:

1. All visitors entering Pretense Flip N.V. facilities must undergo prior authorization.
2. Upon authorized entry, visitors shall be issued a distinct identification badge, clearly distinguishable from employee badges, which must be visibly displayed at all times within the facility.
3. All visitors must be escorted by an Pretense Flip N.V. employee throughout their entire visit within the facility.
4. A visitor log, detailing entry and exit times and visitor information, shall be maintained for all facilities and retained for a minimum period of three (3) to six (6) months.
5. Visitors are required to return their issued identification badges upon departure from the facility.

24.2.2 Personnel Access Control:

1. Employee identification badges and all physical access mechanisms (e.g., access cards, keys) to Pretense Flip N.V. facilities and secure areas shall be immediately revoked upon an individual's termination of employment or contract.
2. All personnel within the facility are responsible for vigilance regarding unbadged individuals or unauthorized persons and are required to challenge or report such observations.

24.3 Defined Security Boundaries & Restricted Areas¹⁰⁵

Pretense Flip N.V. shall clearly define and enforce security boundaries for areas containing sensitive information and critical information processing facilities.

- a) **Authorized Access Only:** Access to these secure areas is strictly limited to authorized personnel.
- b) **Logging:** All entries and exits to secure areas must be logged and monitored.
- c) **Supervision:** Any individual who does not possess explicit authorization to access secure areas must be continuously supervised by authorized personnel while within such areas.
- d) **Prohibition on Recording:** Video recording or photography is strictly prohibited within secure areas without explicit, documented management approval.

24.4 Physical Equipment Protection & Environmental Controls¹⁰⁶

Information processing equipment and related assets must be physically protected against unauthorized access, damage, and environmental threats to ensure their continuous availability, integrity, and confidentiality.

¹⁰⁵ISO 27001 A 7.1.1,A 7.1.2, A 7.2.3, A 11-PCI DSS 9.1,9.2,9.4¹⁰⁶ISO 27001 A 7.1.1- A 7.1.6, A 11.1.1, A 11.1.2-PCI DSS 9.**Secure Siting & Storage:**

1. Equipment must be sited in a manner that prevents unauthorized access.
2. Storage facilities containing sensitive equipment or media must be secured against unauthorized entry.
3. Environmental conditions, such as temperature and humidity, in critical processing facilities (e.g., server rooms, data centres) shall be continuously monitored and maintained within defined acceptable ranges.
4. Appropriate lightning protection measures shall be applied to all Pretense Flip N.V. buildings housing information processing facilities.

Utility Protection & Resilience:

1. Essential information processing equipment must be safeguarded from power failures and other disruptions to supporting utilities (e.g., water, air conditioning, communications). This includes the implementation of uninterruptible power supplies (UPS) and, where critical, redundant power sources.
2. Redundant communication links are required for essential equipment to ensure continuous connectivity.

Maintenance:

1. All IT equipment shall be correctly maintained to ensure its ongoing availability and integrity.
2. All maintenance events, including dates, personnel, and actions taken, must be formally logged.

25 Appendix 1

26 References