

INFORMATION SECURITY POLICY HANDBOOK

Pegasus19 N.V.

Introduction

This Information Security Policy Handbook establishes the framework for protecting the information assets of Pegasus19 ("The Company")

It consolidates all security-related policies into a unified structure to ensure:

- Confidentiality of information
- Integrity of systems and data
- Availability of services
- Compliance with regulatory and industry standards

This handbook is aligned with recognized best practices, including ISO 27001, NIST, and OWASP.

All employees, contractors, and third parties must comply with the policies defined in this document.

Purpose

The purpose of this handbook is to:

- Provide a centralized reference for all security policies
 - Standardize security practices across the organization
 - Reduce operational and security risks
 - Support business continuity and resilience
-

Scope

This handbook applies to:

- All employees
 - Contractors
 - Third parties
 - All systems, applications, infrastructure, and data
-

Policy Structure

This handbook is organized into the following domains:

- 1. Information Security Governance
- 2. Identity and Access Management
- 3. Data Protection and Resilience
- 4. Security Operations
- 5. Secure Development
- 6. Cryptography
- 7. Appendices

Each section contains detailed policies and controls applicable to that domain.

Compliance

Failure to comply with this handbook may result in:

- Disciplinary actions
 - Access revocation
 - Legal consequences
-

Policy Review

This handbook must be reviewed:

- At least annually; or
 - Upon significant changes in business, technology, or regulatory requirements
-

Table of Contents

Section	Policy	Description
1	Information Security Governance	Governance framework and high-level controls
1.1	Information Security Policy	Core security principles and objectives

Section	Policy	Description
1.2	Acceptable Use of Assets Policy	Rules for system and asset usage
1.3	Change Management Policy	Control and management of system changes
2	Identity and Access Management	Access control and identity governance
2.1	Password Management Policy	Password and authentication controls
2.2	Data Classification Policy	Data categorization and protection rules
3	Data Protection and Resilience	Data protection and recovery capabilities
3.1	Backup Policy	Backup strategy and data protection
3.2	Business Continuity Plan (BCP)	Continuity and disaster recovery
4	Security Operations	Operational security processes
4.1	Incident Response Plan	Incident handling and response procedures
5	Secure Development	Secure software practices
5.1	Secure SDLC Policy	Secure development lifecycle controls
6	Cryptography	Cryptographic controls and key management
6.1	Cryptographic Architecture Policy	Encryption and key management
7	Appendices	Supporting information
7.1	Definitions and Glossary	Key terms and definitions
7.2	Policy Review Schedule	Review cycles and ownership
7.3	Compliance Mapping	Alignment with standards (ISO/NIST)

1. INFORMATION SECURITY GOVERNANCE

1.0 Overview

This section defines the governance framework for information security within the Company.

It establishes the policies, principles, and controls required to ensure that information security is managed in a structured, consistent, and effective manner across the organization.

The governance framework ensures that:

- Information security aligns with business objectives
- Risks are identified and managed appropriately
- Responsibilities are clearly defined
- Security policies are implemented and enforced

This section provides the foundation for all other policies within this handbook.

1.1 INFORMATION SECURITY POLICY

1.1.1 Introduction

The Information Security Policy establishes the overarching principles and framework for protecting the information assets of the Company.

It ensures that information is safeguarded against unauthorized access, disclosure, alteration, and destruction while supporting business operations and regulatory compliance.

1.1.2 Objectives

The objectives of this policy are to:

- Ensure confidentiality, integrity, and availability of information
 - Protect systems and data from security threats
 - Support business continuity and operational resilience
 - Ensure compliance with legal, regulatory, and contractual requirements
 - Establish a consistent approach to information security across the organization
-

1.1.3 Scope

This policy applies to:

- All employees
- Contractors

- Third parties
- All information assets, including systems, applications, infrastructure, and data

It covers all environments, including:

- On-premises systems
 - Cloud services
 - Remote access environments
-

1.1.4 Information Security Principles

1.1.4.1 Confidentiality

Information must be accessible only to authorized individuals and protected against unauthorized disclosure.

1.1.4.2 Integrity

Information must be accurate, complete, and protected against unauthorized modification.

1.1.4.3 Availability

Information and systems must be available when required to support business operations.

1.1.5 Governance and Responsibilities

Information security is a shared responsibility across the organization.

Management is responsible for:

- Establishing and enforcing security policies
- Providing resources for implementation
- Ensuring alignment with business objectives

Employees and users are responsible for:

- Protecting information assets
 - Complying with security policies
 - Reporting security incidents or suspicious activities
-

1.1.6 Risk Management

The Company adopts a risk-based approach to information security.

Security controls must be:

- Proportional to the level of risk
 - Regularly reviewed and updated
 - Designed to mitigate identified threats and vulnerabilities
-

1.1.7 Compliance

All activities must comply with:

- Applicable laws and regulations
- Industry standards
- Internal policies and procedures

Non-compliance may result in:

- Disciplinary actions
 - Legal consequences
-

1.1.8 Policy Review

This policy must be reviewed:

- At least annually; or
- Whenever significant changes occur in:
 - Technology
 - Business processes
 - Regulatory requirements

Updates must be approved and communicated to relevant stakeholders.

1.2 ACCEPTABLE USE OF ASSETS POLICY

1.2.1 Introduction

This policy defines the acceptable use of information systems, assets, and resources within the Company.

It ensures that all users understand their responsibilities when accessing and using organizational assets, minimizing risks related to misuse, security breaches, and operational disruptions.

1.2.2 Scope

This policy applies to:

- All employees
- Contractors
- Third parties

It covers all company assets, including:

- Computers and mobile devices
 - Networks and infrastructure
 - Applications and systems
 - Internet and email usage
-

1.2.3 Acceptable Use

Users are permitted to:

- Use company systems for authorized business purposes
- Access only systems and data they are authorized to use
- Communicate professionally and responsibly using company resources

Limited personal use may be allowed provided that it:

- Does not interfere with business operations
 - Does not violate any policies
 - Does not introduce security risks
-

1.2.4 Prohibited Use

Users must not:

- Access systems or data without authorization
 - Share credentials or allow others to use their accounts
 - Install unauthorized software or tools
 - Use company assets for illegal or unethical activities
 - Attempt to bypass security controls
 - Introduce malicious software or unsafe content
-

1.2.5 User Responsibilities

All users must:

- Protect their authentication credentials
- Lock devices when unattended

- Follow all security policies and procedures
- Report any suspected security incidents immediately

Users are accountable for all actions performed using their assigned accounts.

1.2.6 Monitoring and Privacy

All usage of company systems may be:

- Logged
- Monitored
- Audited

This is performed to:

- Ensure security
- Detect misuse
- Maintain compliance

Users should not expect privacy when using company-owned systems.

1.2.7 Enforcement

Violations of this policy may result in:

- Disciplinary actions
 - Access revocation
 - Legal consequences
-

1.2.8 Policy Review

This policy must be reviewed:

- At least annually; or
- When significant changes occur in technology, risks, or business operations

Updates must be communicated to all users.

1.3 CHANGE MANAGEMENT POLICY

1.3.1 Introduction

The Company recognizes the importance of maintaining a secure and controlled IT environment, ensuring the integrity, availability, and confidentiality of systems and data.

To achieve these objectives, a structured and disciplined approach to implementing changes in information systems and IT infrastructure is required.

This policy ensures that all changes are:

- Performed in a secure manner
 - Properly documented
 - Designed to minimize operational and security risks
-

1.3.2 Scope

This policy applies to all changes affecting:

- Information systems
- IT infrastructure
- Related services

It covers the entire lifecycle of changes, including:

- Request
- Impact analysis
- Approval
- Implementation
- Monitoring
- Post-implementation review

All employees, partners, and third parties must comply with this policy.

1.3.3 Roles and Responsibilities

1.3.3.1 Change Management Team

Responsible for:

- Overseeing the change management process
 - Approving high-impact changes
 - Ensuring alignment with business and security objectives
 - Monitoring performance and compliance
 - Conducting post-implementation reviews
-

1.3.3.2 Change Requester

Responsible for:

- Defining the change and its objectives
 - Providing justification and expected benefits
 - Performing initial impact assessment
 - Supporting evaluation and approval processes
-

1.3.3.3 System or Service Owner

Responsible for:

- Evaluating technical and operational impacts
 - Approving or rejecting changes
 - Ensuring readiness for implementation
 - Validating outcomes
-

1.3.3.4 Implementation Team

Responsible for:

- Executing approved changes
 - Ensuring backup and recovery readiness
 - Performing testing
 - Documenting implementation details
 - Reporting outcomes
-

1.3.3.5 Information Security Team

Responsible for:

- Assessing security risks
 - Ensuring mitigation measures
 - Approving changes from a security perspective
-

1.3.4 Change Classification

1.3.4.1 Standard Changes

Low-risk, pre-approved changes with established procedures.

1.3.4.2 Normal Changes

Require full assessment and approval before implementation.

1.3.4.3 Emergency Changes

Require immediate action but must still follow defined procedures with post-review.

1.3.5 Change Management Process

1.3.5.1 Change Request Submission

All change requests must include:

- Detailed description
 - Justification
 - Impact analysis
 - Proposed schedule
-

1.3.5.2 Impact and Risk Assessment

All changes must be evaluated for:

- Technical impact
- Operational impact
- Security risks

Mitigation measures must be defined.

1.3.5.3 Change Approval

Changes must be approved by:

- Change Management Team
- System Owner
- Information Security Team

Final approval must be formally documented.

1.3.6 Implementation and Deployment

1.3.6.1 Scheduling

Changes must be scheduled to minimize disruption.

1.3.6.2 Execution

Implementation must follow the approved plan without deviation.

1.3.6.3 Communication

All stakeholders must be informed prior to implementation.

1.3.7 Testing and Validation

All changes must be tested in a controlled environment before production deployment.

Testing must ensure:

- Functionality
 - Security
 - Compatibility
-

1.3.8 Backup and Recovery

1.3.8.1 Backup Requirements

A full backup must be performed before any change.

1.3.8.2 Recovery Capability

Recovery procedures must be available to restore systems if needed.

1.3.9 Documentation and Tracking

All changes must be:

- Logged
- Tracked
- Documented

This ensures traceability and accountability.

1.3.10 Post-Implementation Review

A review must be conducted after implementation to:

- Confirm success
 - Identify issues
 - Improve future processes
-

1.3.11 Emergency Changes

Emergency changes must:

- Follow an accelerated process
 - Still include documentation, testing, and approval
 - Be reviewed after implementation
-

1.3.12 Policy Review

This policy must be reviewed:

- Annually; or
 - When significant changes occur
-

2. IDENTITY AND ACCESS MANAGEMENT

2.0 Overview

This section defines the principles and controls for managing identities and access to systems, applications, and data within the Company.

It ensures that:

- Access is granted based on business need
- Users are properly authenticated and authorized
- Sensitive information is protected from unauthorized access
- Identity lifecycle is managed securely

The controls defined in this section support:

- Protection of critical systems and data
 - Enforcement of the principle of least privilege
 - Compliance with regulatory and security requirements
-

2.1 PASSWORD MANAGEMENT POLICY

2.1.1 Introduction

The improper creation and use of passwords can compromise the security of corporate resources, resulting in:

- Unauthorized access

- Data leakage
- Damage to organizational integrity

This policy establishes guidelines for the creation, use, and management of passwords to ensure alignment with security best practices and regulatory requirements.

2.1.2 Scope

This policy applies to:

- Employees
- Contractors
- Service providers
- Partners

It covers access to:

- Internal systems
 - External systems
 - Remote environments
 - Physical and logical access where applicable
-

2.1.3 User Identification and Authentication

Each user must have a unique identity for system access, consisting of:

- Username
- Password

Passwords are a critical authentication mechanism used to verify user identity and protect system access.

2.1.4 Password Requirements

2.1.4.1 Minimum Length

Passwords must contain at least 8 characters.

2.1.4.2 Complexity

Passwords must include a combination of:

- Uppercase letters
- Lowercase letters

- Numbers
- Special characters

2.1.4.3 Password Rotation

Passwords must be changed at least every 90 days.

2.1.5 Password Change and Reuse

2.1.5.1 Expiration Control

Systems must:

- Notify users before password expiration
- Enforce timely password updates

2.1.5.2 Reuse Restrictions

Passwords must not be reused.

Systems must:

- Store password history (minimum last 4 passwords)
 - Prevent reuse of stored passwords
-

2.1.6 Multi-Factor Authentication (MFA)

MFA must be implemented for:

- Critical systems
- Remote access
- Sensitive data access

Authentication mechanisms must align with the Access & Identity Management controls.

2.1.7 Credential Confidentiality

Passwords must:

- Be kept confidential
- Not be shared under any circumstances

If a password is suspected to be compromised:

- It must be changed immediately

- The Information Security team must be notified
-

2.1.8 Password Storage

Passwords must not be:

- Written down
- Stored in emails or notes
- Stored on unsecured devices

Approved storage:

- Passwords may only be stored using an approved password manager
 - The approved solution is PassBolt (or equivalent)
-

2.1.9 Secure Distribution of Credentials

Authentication information (e.g., temporary passwords, tokens) must be:

- Generated securely
- Unique per user
- Protected against reuse and interception

Unencrypted communication must not be used for credential transmission.

2.1.10 Identity Verification

Before performing authentication changes (e.g., password reset), identity must be verified using secure methods such as:

- MFA
 - Predefined verification processes
 - Secure authentication mechanisms
-

2.1.11 Prohibited Practices

The following are strictly prohibited:

- Password sharing
 - Use of weak or predictable passwords
 - Use of compromised credentials
 - Transmission of passwords via unsecured channels
-

2.1.12 User Guidance and Best Practices

Users must be encouraged to:

- Avoid predictable passwords
- Use password generators
- Use passphrases (e.g., multiple random words)

Security controls must balance:

- Strong protection
 - Usability
-

2.1.13 Roles and Responsibilities

2.1.13.1 End Users

Responsible for:

- Maintaining secure passwords
 - Not sharing credentials
 - Reporting suspected compromise
-

2.1.13.2 IT Team

Responsible for:

- Enforcing password controls
 - Managing authentication systems
 - Monitoring access logs
 - Disabling compromised or inactive accounts
-

2.1.13.3 Information Security Manager

Responsible for:

- Reviewing policy effectiveness
 - Ensuring compliance with standards
 - Managing credential-related incidents
 - Conducting audits
-

2.1.14 Monitoring and Logging

All access and authentication attempts must be:

- Logged
- Monitored

Compromised credentials must be:

- Disabled immediately
-

2.1.15 Policy Review

This policy must be reviewed:

- At least annually; or
 - When required by regulatory or operational changes
-

2.2 DATA CLASSIFICATION POLICY

2.2.1 Introduction

The Data Classification Policy defines guidelines for the classification, protection, and management of data within the Company.

These guidelines ensure the:

- Confidentiality
- Integrity
- Availability

of information and establish a structured approach for handling sensitive and critical data.

2.2.2 Scope

This policy applies to:

- Employees
- Third parties
- Suppliers
- Systems and applications

It covers all data that is:

- Accessed
- Processed
- Stored

within the organization.

2.2.3 Data Classification Model

All data must be classified based on its sensitivity and importance.

2.2.3.1 Public Data

Information that may be disclosed without restriction.

Examples:

- Marketing materials
 - Public documentation
-

2.2.3.2 Internal Data

Information intended for internal use only.

Examples:

- Internal procedures
 - Corporate communications
-

2.2.3.3 Restricted Data

Information accessible to a limited group and requiring enhanced protection.

Examples:

- Business strategies
 - Contracts
 - Internal reports
-

2.2.3.4 Sensitive Data

Information requiring additional protection due to regulatory or business impact.

Examples:

- Personal data
 - Financial transactions
-

2.2.3.5 Confidential Data

Highly sensitive information that could cause severe damage if exposed.

Examples:

- Credentials
 - Encryption keys
 - Critical backups
 - Audit logs
-

2.2.4 Classification Criteria

Data classification must consider:

- Sensitivity
 - Business criticality
 - Regulatory requirements
 - Data lifecycle
-

2.2.4.1 Data Sensitivity

Data must be evaluated based on the potential impact of unauthorized disclosure.

Sensitive and confidential data must be protected with:

- Strong access controls
 - Encryption
 - Multi-Factor Authentication (MFA)
-

2.2.4.2 Business Criticality

Data must be classified according to its importance to business operations.

Critical data must be protected with:

- Backup mechanisms
 - Secure storage
 - Disaster recovery plans
-

2.2.4.3 Regulatory Requirements

Classification must reflect applicable legal and regulatory obligations.

Data subject to regulation must:

- Be properly classified

- Have additional controls applied
-

2.2.4.4 Data Lifecycle and Accessibility

Classification must consider:

- Access requirements
- Retention periods

Access must be:

- Restricted
 - Periodically reviewed
-

2.2.5 Data Labeling and Identification

All data must be clearly identified according to its classification.

2.2.5.1 Digital Data

Digital data must be labeled using:

- Tags
 - System classifications
-

2.2.5.2 Physical Documents

Physical documents containing restricted, sensitive, or confidential data must:

- Be clearly labeled
 - Include handling instructions
-

2.2.5.3 Classification Responsibility

Data owners and creators must:

- Assign classification
 - Ensure correct labeling
-

2.2.5.4 Periodic Review

Classifications must be reviewed periodically to ensure accuracy.

2.2.6 Access Control and Authentication

Access to data must follow:

- Principle of Least Privilege
 - Role-based access controls
-

2.2.6.1 Multi-Factor Authentication

MFA must be used for:

- Sensitive data
 - Critical systems
 - Remote access
-

2.2.6.2 Access Restriction

Access to restricted, sensitive, and confidential data must:

- Be controlled
 - Be approved
 - Be periodically reviewed
-

2.2.6.3 Access Logging

All access must be:

- Logged
- Monitored

Logs must be reviewed to detect:

- Unauthorized access
 - Suspicious activity
-

2.2.7 Data Protection Controls

Data must be protected according to its classification.

2.2.7.1 Storage Security

Data must be stored in environments with appropriate access controls.

2.2.7.2 Encryption

Sensitive and confidential data must be encrypted:

- At rest
 - In transit
-

2.2.7.3 Monitoring

All access to protected data must be monitored.

2.2.8 Data Retention and Disposal

2.2.8.1 Retention

Data must be retained only for the required period based on classification and business needs.

2.2.8.2 Secure Disposal

Data must be securely destroyed when no longer needed.

Methods include:

- Secure deletion
- Physical destruction

Disposal must ensure data cannot be recovered.

2.2.9 Backup and Recovery

Data must be protected through:

- Regular backups
- Redundant storage
- Disaster recovery mechanisms

Backup practices must align with the Backup Policy.

2.2.10 Roles and Responsibilities

2.2.10.1 Information Security Manager

Responsible for:

- Policy enforcement
 - Compliance monitoring
 - Incident oversight
-

2.2.10.2 IT Team

Responsible for:

- Implementing controls
 - Managing access
 - Performing backups
 - Testing data availability
-

2.2.10.3 Data Owners

Responsible for:

- Classifying data
 - Ensuring proper handling
 - Reviewing access
-

2.2.10.4 Employees

Responsible for:

- Following classification rules
 - Protecting data
 - Reporting incidents
-

2.2.11 Policy Review

This policy must be reviewed:

- At least annually; or
 - When regulatory or business changes occur
-

3. DATA PROTECTION AND RESILIENCE

3.0 Overview

This section defines the controls and strategies required to protect data and ensure the resilience of systems and services within the Company.

It establishes mechanisms to:

- Protect data against loss, corruption, or unauthorized access
- Ensure availability of critical information
- Support recovery from failures and disasters
- Maintain operational continuity under adverse conditions

The controls in this section align with business continuity, disaster recovery, and data protection requirements to ensure that critical operations can be restored within acceptable timeframes.

3.1 BACKUP POLICY

3.1.1 Introduction

This policy defines the guidelines and procedures required to ensure the protection, integrity, and availability of data within the Company.

It ensures:

- Business continuity
- Minimization of data loss
- Reduction of system downtime

in the event of failures or disasters.

3.1.2 Scope

This policy applies to all systems and data used in the operations of the Company, including:

- Application platforms and operational systems
- Databases, logs, and configuration data
- Infrastructure components and storage systems
- Third-party systems and cloud services

All personnel and service providers must comply with this policy.

3.1.3 Backup Strategy

3.1.3.1 Scope and Coverage

All critical systems and data must be included in backup processes, including:

- Operational systems
 - User data
 - Transaction records
 - Security and audit logs
-

3.1.3.2 Critical Data Identification

Data must be classified based on importance and business impact.

Critical data must receive:

- Higher backup frequency
 - Enhanced protection
 - Priority recovery
-

3.1.4 Backup Frequency and Scheduling

3.1.4.1 Backup Frequency

A full backup must be performed daily for critical systems.

3.1.4.2 Scheduling

Backups should be executed:

- Outside peak operational hours; or
 - At the end of each operational cycle
-

3.1.4.3 Automation and Monitoring

Backup processes must be:

- Automated
- Actively monitored

to ensure:

- Successful execution
 - Data integrity
-

3.1.5 Storage and Redundancy

3.1.5.1 Primary Storage

Backup data is stored using resilient infrastructure distributed across multiple availability zones.

3.1.5.2 Geographic Redundancy

Backups must be replicated to geographically separate locations to ensure:

- Protection against regional failures
 - High availability
-

3.1.5.3 Cross-Platform Resilience

Backup copies may be maintained across different platforms to:

- Reduce dependency on a single provider
 - Improve disaster recovery capabilities
-

3.1.6 Data Retention

3.1.6.1 Retention Period

Backup data must be retained according to:

- Business requirements
- Regulatory obligations

Critical records (e.g., audit and security data) must be retained for extended periods as required.

3.1.6.2 Storage Lifecycle

Data must be managed using a lifecycle approach:

- Short-term storage for immediate access
 - Long-term storage for archival purposes
-

3.1.7 Backup and Recovery

3.1.7.1 Recovery Capability

Systems must be capable of restoring data from the most recent valid backup.

3.1.7.2 Integrity Verification

Backup integrity must be validated through:

- Periodic restore testing
 - System recovery simulations
-

3.1.7.3 Infrastructure Resilience

Backup infrastructure must support:

- Redundant components
 - Automatic recovery mechanisms
 - Rapid synchronization after restoration
-

3.1.8 Encryption and Security

3.1.8.1 Encryption

Backup data must be protected using strong encryption:

- At rest
 - In transit
-

3.1.8.2 Access Control

Access to backups must be:

- Restricted to authorized personnel
 - Protected using strong authentication (e.g., MFA)
-

3.1.8.3 Monitoring and Logging

All access to backup systems must be:

- Logged
 - Monitored
-

3.1.9 Audit and Review

3.1.9.1 Audit

Regular audits must verify that:

- Backup procedures are followed

- Data is properly protected
-

3.1.9.2 Risk Assessment

Periodic risk assessments must identify:

- New threats
 - Vulnerabilities
 - Required improvements
-

3.1.10 Roles and Responsibilities

3.1.10.1 IT Team

Responsible for:

- Executing backups
 - Monitoring processes
 - Resolving failures
 - Performing recovery tests
-

3.1.10.2 Information Security Manager

Responsible for:

- Ensuring data protection
 - Reviewing backup practices
 - Conducting audits
-

3.1.10.3 Third Parties

Must:

- Comply with backup requirements
 - Provide evidence of compliance
-

3.1.11 Policy Review

This policy must be reviewed:

- At least annually; or
 - When significant changes occur
-

3.2 BUSINESS CONTINUITY PLAN (BCP)

3.2.1 Introduction

The Business Continuity Plan (BCP) establishes the framework required to ensure that the Company can continue critical operations during and after disruptive events.

The plan ensures:

- Effective response to incidents
- Minimization of operational impact
- Restoration of services within acceptable timeframes

Business continuity is a continuous process requiring regular evaluation, testing, and improvement.

3.2.2 Scope

This plan applies to:

- All business units
- All critical systems and processes
- Employees, contractors, and third parties

It covers:

- Operational disruptions
 - Technology failures
 - Cybersecurity incidents
 - Natural disasters
-

3.2.3 Objectives

The objectives of the BCP are to:

- Maintain continuity of critical operations
 - Reduce the impact of disruptions
 - Ensure timely recovery of services
 - Protect organizational assets and reputation
-

3.2.4 Business Continuity Management (BCM)

3.2.4.1 BCM Lifecycle

The Business Continuity Management program follows a continuous lifecycle:

- Plan – Define strategies and procedures
 - Do – Implement continuity measures
 - Check – Monitor and test effectiveness
 - Act – Improve and update processes
-

3.2.4.2 Governance

Senior management must:

- Support the BCM program
 - Provide necessary resources
 - Ensure alignment with business objectives
-

3.2.5 Business Impact Analysis (BIA)

3.2.5.1 Critical Process Identification

All critical business processes must be identified and prioritized.

3.2.5.2 Impact Assessment

Impacts must be evaluated across:

- Financial
 - Operational
 - Reputational
 - Legal and regulatory
-

3.2.5.3 Time-Based Metrics

The following recovery metrics must be defined:

- MTD (Maximum Tolerable Downtime)
 - RTO (Recovery Time Objective)
 - RPO (Recovery Point Objective)
-

3.2.6 Risk Assessment

3.2.6.1 Threat Identification

Potential threats include:

- Cyberattacks
 - Infrastructure failures
 - Human error
 - Natural disasters
-

3.2.6.2 Risk Evaluation

Risks must be evaluated based on:

- Likelihood
 - Impact
 - Business criticality
-

3.2.7 Business Continuity Strategies

3.2.7.1 Technology

Strategies include:

- Redundant systems
 - Geographic distribution
 - Failover mechanisms
-

3.2.7.2 Data

Data must be protected through:

- Backup processes
 - Replication
 - Secure storage
-

3.2.7.3 People

Measures must include:

- Cross-training
 - Role redundancy
 - Succession planning
-

3.2.7.4 Facilities

Facilities strategies include:

- Alternative sites

- Remote work capabilities
-

3.2.7.5 Suppliers

Third-party dependencies must be:

- Assessed
 - Monitored
 - Supported with contingency plans
-

3.2.8 Incident Response Integration

The BCP must operate in alignment with:

- Incident Response Plan
 - Disaster Recovery procedures
-

3.2.9 Response and Recovery

3.2.9.1 Incident Response

The organization must:

- Identify and assess incidents
 - Contain and control impact
 - Coordinate response activities
-

3.2.9.2 Recovery

Recovery procedures must ensure:

- Restoration of systems
 - Validation of data integrity
 - Resumption of operations
-

3.2.9.3 Communication

Communication must be:

- Timely
- Accurate
- Coordinated

It must include:

- Internal stakeholders
 - External parties (if required)
-

3.2.10 Testing and Maintenance

3.2.10.1 Testing

BCP testing must include:

- Tabletop exercises
 - Simulations
 - Full recovery tests
-

3.2.10.2 Frequency

Testing must be conducted:

- Periodically
 - After significant changes
 - After incidents
-

3.2.10.3 Continuous Improvement

Improvements must be based on:

- Test results
 - Incident lessons learned
 - Risk changes
-

3.2.11 Roles and Responsibilities

3.2.11.1 Management

Responsible for:

- Approving strategies
 - Providing resources
-

3.2.11.2 IT and Operations

Responsible for:

- Implementing recovery solutions
- Maintaining systems

3.2.11.3 Information Security

Responsible for:

- Ensuring alignment with security policies
 - Supporting incident handling
-

3.2.12 Plan Activation

The BCP may be activated in cases such as:

- System failures
- Cyber incidents
- Infrastructure disruptions
- Natural disasters

Activation must be:

- Clearly defined
 - Documented
 - Communicated
-

3.2.13 Monitoring and Review

The BCP must be:

- Monitored continuously
- Reviewed periodically

Reviews must ensure:

- Accuracy
 - Effectiveness
 - Alignment with business needs
-

3.2.14 Policy Review

This plan must be reviewed:

- At least every 2 years; or
 - After significant changes or incidents
-

4. Security Operations

4.0 Overview

The Security Operations domain defines the processes and procedures required to detect, respond to, and manage information security and privacy incidents within the Company.

It ensures that:

- Security events are identified in a timely manner
- Incidents are properly analyzed and contained
- Impacts are minimized
- Systems and operations are restored efficiently

This domain supports continuous monitoring, structured incident handling, and ongoing improvement of the organization's security posture.

4.1 Incident Response Plan

4.1.1 Introduction

This Incident Response Plan establishes the methodology for identifying, managing, and responding to security and privacy incidents.

The plan ensures:

- Timely detection and response
 - Protection of data and systems
 - Compliance with regulatory requirements
 - Structured and documented incident handling
-

4.1.2 Scope

This plan applies to:

- All employees
- Contractors
- Third parties

It covers:

- Information security incidents
- Privacy and personal data incidents
- System and operational disruptions

4.1.3 Definitions

Key concepts include:

- Information Security Incident – Event affecting confidentiality, integrity, or availability
 - Privacy Incident – Breach involving personal data
 - Vulnerability – Weakness that may be exploited
 - Impact – Severity of incident consequences
 - Mitigation – Actions to reduce damage
 - Recovery – Restoration of systems and operations
-

4.1.4 Roles and Responsibilities

4.1.4.1 Information Security Committee

Responsible for:

- Coordinating incident response
 - Overseeing investigations
 - Ensuring proper handling of evidence
 - Reporting to management
-

4.1.4.2 Data Protection Officer (DPO)

Responsible for:

- Managing personal data incidents
 - Determining regulatory notification requirements
 - Acting as liaison with authorities
-

4.1.4.3 Incident Response Team (IRT)

Responsible for:

- Detection and analysis
 - Containment and eradication
 - Recovery actions
 - Documentation
-

4.1.4.4 Employees

Responsible for:

- Reporting incidents immediately
 - Supporting investigations
 - Following security procedures
-

4.1.5 Proactive Security Practices

The organization must:

- Maintain monitoring systems
 - Ensure effectiveness of detection tools
 - Securely store incident evidence
 - Maintain incident response tools and infrastructure
-

4.1.6 Incident Communication

Communication must ensure:

- Timely escalation
- Coordination between teams
- Notification of stakeholders

Includes:

- Internal escalation
 - Executive notification
 - Third-party communication
 - Regulatory communication (if required)
-

4.1.7 Incident Management Lifecycle

4.1.7.1 Preparation

Includes:

- Policies and procedures
 - Training and awareness
 - Monitoring tools
 - Communication channels
-

4.1.7.2 Detection and Analysis

Includes:

- Identification of suspicious events

- Validation of incidents
 - Classification and impact assessment
 - Evidence preservation
-

4.1.7.3 Containment, Eradication, and Recovery

Containment

- Isolate affected systems
- Prevent spread

Eradication

- Remove root cause
- Apply patches and fixes

Recovery

- Restore systems from backups
 - Validate system integrity
 - Reinforce security controls
-

4.1.7.4 Post-Incident Activities

Includes:

- Documentation
 - Root cause analysis
 - Lessons learned
 - Improve future processes
-

4.1.8 Incident Classification

4.1.8.1 Categories

Incidents may include:

- Unauthorized access
 - Data exposure
 - Malware / ransomware
 - Phishing
 - DoS / DDoS
 - System failures
 - Human error
-

4.1.8.2 Impact Levels

- P1 – Critical
 - P2 – High
 - P3 – Medium
 - P4 – Low
-

4.1.8.3 SLA (Response Time)

- P1 – 4 hours
 - P2 – 8 hours
 - P3 – 36 hours
 - P4 – 48 hours
-

4.1.9 Incident Handling Procedures

All incidents must follow:

1. Identification and recording
 2. Classification and prioritization
 3. Containment and mitigation
 4. Eradication of root cause
 5. Recovery of systems
 6. Documentation and closure
-

4.1.10 Evidence Handling

Evidence must be:

- Collected securely
 - Preserved in original state
 - Documented and traceable
-

4.1.11 Incident Reporting

All incidents must be:

- Logged in tracking systems
- Documented with full details
- Reported to relevant stakeholders

Reports must include:

- Timeline
- Impact

- Actions taken
 - Resolution
-

4.1.12 External Communication

When required:

- Regulatory authorities must be notified
- Affected individuals must be informed
- Third parties must be engaged

All communication must be:

- Approved
 - Accurate
 - Controlled
-

4.1.13 Monitoring and Continuous Improvement

The organization must:

- Analyze incident trends
 - Improve controls
 - Update procedures
 - Conduct periodic reviews
-

4.1.14 Policy Review

This plan must be reviewed:

- Annually; or
 - After major incidents or changes
-

5. Secure Development

5.0 Overview

The Secure Development domain establishes the principles and controls required to ensure that security is embedded throughout the software development lifecycle (SDLC).

It ensures that:

- Applications are developed securely

- Vulnerabilities are minimized
- Changes are controlled and traceable
- Systems maintain integrity and compliance

This domain supports the delivery of secure, reliable, and resilient software solutions.

5.1 Secure Software Development Lifecycle (SDLC) Policy

5.1.1 Introduction

This policy defines structured guidelines for secure software development within the Company. It ensures that all development activities:

- Follow secure coding practices
 - Address risks early in the lifecycle
 - Comply with security and regulatory requirements
-

5.1.2 Scope

This policy applies to:

- All development teams
- Contractors and third parties
- All applications and systems

It covers:

- New development
 - Maintenance
 - Updates and patches
-

5.1.3 Roles and Responsibilities

5.1.3.1 Security Manager

Responsible for:

- Ensuring security is integrated into SDLC
 - Defining security requirements
 - Overseeing compliance
-

5.1.3.2 Development Manager

Responsible for:

- Managing development processes
 - Ensuring adherence to secure practices
 - Approving code changes and deployments
-

5.1.3.3 Developers

Responsible for:

- Writing secure code
 - Performing code reviews
 - Following development standards
-

5.1.4 Secure Development Principles

5.1.4.1 Security by Design

Security must be integrated from:

- Requirements phase
- Design phase
- Development and testing

Includes:

- Risk assessments
 - Early vulnerability identification
-

5.1.4.2 Security Standards

Development must align with:

- OWASP guidelines
 - NIST recommendations
 - ISO/IEC 27001 principles
-

5.1.4.3 Security Reviews

Regular reviews must be conducted to:

- Identify vulnerabilities
 - Apply corrective actions
 - Improve development practices
-

5.1.5 Environment Segregation

5.1.5.1 Environment Separation

Environments must be:

- Physically and logically separated
 - Segmented (development, testing, production)
-

5.1.5.2 Data Protection

Production data must:

- Not be used in development/testing
 - Be replaced with anonymized or fictitious data
-

5.1.5.3 Production Access

Access to production must be:

- Restricted
- Granted only to authorized personnel

Developers must not have direct production access.

5.1.6 Access Control in Development

5.1.6.1 Least Privilege

Access must follow:

- Principle of least privilege
-

5.1.6.2 Access Approval

All access must be:

- Approved
 - Documented
 - Traceable
-

5.1.6.3 Privileged Access

Privileged access must:

- Limited
 - Require strong authentication (e.g., MFA)
 - Be monitored
-

5.1.7 Change Control and Versioning

5.1.7.1 Version Control

All code must be managed through:

- Version control systems (e.g., Git)
-

5.1.7.2 Branching and Review

- Be developed in separate branches
 - Undergo code review (pull requests)
-

5.1.7.3 Deployment Control

Changes must:

- Be tested before production
 - Be formally approved
 - Follow change management procedures
-

5.1.7.4 Rollback

All changes must include:

- Rollback procedures
 - Tested recovery mechanisms
-

5.1.8 Vulnerability and Incident Management

5.1.8.1 Incident Handling

Incidents in development must:

- Be reported immediately
 - Follow the Incident Response Plan
-

5.1.8.2 Vulnerability Management

Vulnerabilities must be:

- Identified
 - Assessed by risk level
 - Prioritized for remediation
-

5.1.8.3 Patch Management

Critical vulnerabilities must:

- Be patched immediately
 - Be tested before deployment
-

5.1.8.4 Validation

After remediation:

- Security testing must confirm resolution
 - No new vulnerabilities are introduced
-

5.1.9 Monitoring and Logging

All development activities must be:

- Logged
- Monitored

Logs must support:

- Traceability
 - Audit requirements
-

5.1.10 Policy Review

This policy must be reviewed:

- Annually; or
- After significant changes

Updates must be:

- Documented
 - Communicated to relevant teams
-

6. Cryptography

6.0 Overview

The Cryptography domain defines the standards and controls required to protect sensitive and confidential data through the use of encryption and secure key management.

It ensures that:

- Data is protected in transit and at rest
- Cryptographic keys are securely managed
- Secure communication protocols are enforced
- Risks related to data exposure and interception are minimized

This domain supports the confidentiality, integrity, and trustworthiness of all information processed within the Company.

6.1 Cryptographic Architecture Policy

6.1.1 Introduction

This policy establishes the principles and controls for the use of cryptography within the Company.

It ensures that:

- Sensitive and confidential data is protected
 - Cryptographic mechanisms are properly implemented
 - Security risks related to encryption are minimized
-

6.1.2 Scope

This policy applies to:

- All systems handling sensitive data
- All cryptographic processes
- Employees, contractors, and third parties

It covers:

- Data encryption
 - Secure communications
 - Cryptographic key management
-

6.1.3 General Cryptographic Principles

All sensitive data must be:

- Protected using strong encryption
- Accessible only by authorized users

Cryptographic controls must ensure:

- Confidentiality
- Integrity
- Availability

Cryptographic methods must be:

- Periodically reviewed
 - Aligned with industry standards
-

6.1.4 Access Control and Authentication

6.1.4.1 Authentication for Encrypted Data

Access to encrypted data must require:

- Strong authentication
 - Preferably Multi-Factor Authentication (MFA)
-

6.1.4.2 Credential and Key Protection

Credentials and keys must be:

- Stored securely (e.g., key vaults)
- Protected with encryption

They must not be:

- Hardcoded in applications
 - Exposed in plaintext
-

6.1.4.3 Privilege Management

Access must follow:

- Principle of least privilege

Segregation of duties must be enforced to:

- Prevent misuse of cryptographic assets
- Logged
- Auditable

6.1.5 Communication Security

6.1.5.1 Encryption in Transit

- TLS 1.2 or higher
 - VPN or equivalent secure channels
-

6.1.5.2 Secure Protocols

- HTTPS
- SSH
- SFTP

Outdated or insecure protocols must be:

- Disabled
 - Replaced
-

6.1.5.3 Protection Against Interception

Communication must include:

- Mutual authentication
- Certificate validation

to prevent:

- Man-in-the-middle attacks
-

6.1.6 Storage Encryption

6.1.6.1 Encryption at Rest

Sensitive and confidential data must be encrypted at rest using:

- Strong algorithms (e.g., AES-256)
-

6.1.6.2 Data Integrity

Mechanisms must ensure:

- Protection against unauthorized modification
- Verification of data integrity

6.1.7 Cryptographic Key Management

6.1.7.1 Key Access Control

- Restricted
 - Limited to authorized personnel
-

6.1.7.2 Key Storage

Keys must be:

- Stored securely
- Encrypted
- Segregated from data

Redundant storage must be implemented to ensure:

- Availability
 - Resilience
-

6.1.7.3 Key Lifecycle Management

Keys must be:

- Generated securely
 - Rotated periodically
 - Revoked when compromised or no longer needed
-

6.1.7.4 Monitoring and Audit

All key usage must be:

- Logged
- Monitored

Alerts must be generated for:

- Unauthorized access
 - Suspicious activity
-

6.1.8 Cryptographic Incident Response

In case of compromise:

- Affected keys must be revoked immediately
- New keys must be issued

The incident must:

- Be investigated
- Follow the Incident Response Plan

Corrective actions must:

- Prevent recurrence
 - Strengthen controls
-

6.1.9 Policy Review

This policy must be reviewed:

- Annually; or
- After significant changes affecting cryptographic controls

Updates must be:

- Documented
 - Approved
 - Communicated
-

7. Appendices

7.0 Overview

The Appendices section provides supporting information for the Information Security Handbook, including definitions, governance structures, review schedules, and compliance mappings.

It ensures:

- Consistent understanding of terminology
 - Clear policy maintenance processes
 - Alignment with regulatory and industry standards
-

7.1 Definitions and Glossary

The following terms are used throughout this handbook:

Access Control

The process of granting or restricting access to systems, data, and resources.

Authentication

The process of verifying the identity of a user or system.

Authorization

The process of granting permissions to access resources after authentication.

Availability

Ensuring that systems and data are accessible when needed.

Backup

A copy of data stored separately to enable recovery after failure or loss.

Confidentiality

Protection of information from unauthorized access or disclosure.

Data Integrity

Ensuring that data remains accurate and unaltered.

Encryption

The process of converting data into a secure format to prevent unauthorized access.

Incident

Any event that compromises or threatens the security of systems or data.

Least Privilege

Principle where users are granted only the minimum access required.

Multi-Factor Authentication (MFA)

Authentication method requiring two or more verification factors.

Recovery Time Objective (RTO)

Maximum acceptable time to restore a system after disruption.

Recovery Point Objective (RPO)

Maximum acceptable data loss measured in time.

Risk

Potential for loss or damage when a threat exploits a vulnerability.

Vulnerability

A weakness that can be exploited by a threat.

7.2 Policy Review Schedule

All policies within this handbook must be reviewed to ensure continued effectiveness, relevance, and compliance.

7.2.1 Review Frequency

- All policies must be reviewed at least **annually**
 - Critical policies (e.g., Incident Response, BCP) should be reviewed **after major incidents**
 - Policies must be reviewed when:
 - Regulatory requirements change
 - Business processes change
 - Technology changes significantly
-

7.2.2 Review Responsibilities

- Information Security Manager – overall coordination
 - Policy Owners – content accuracy and updates
 - Senior Management – approval of changes
-

7.2.3 Review Process

The review process must include:

1. Evaluation of policy effectiveness
 2. Identification of gaps or outdated controls
 3. Updates based on risks and regulatory changes
 4. Documentation of changes
 5. Communication to stakeholders
-

7.3 Compliance Mapping

This handbook aligns with recognized standards and frameworks to ensure compliance and best practices.

7.3.1 ISO/IEC 27001 Alignment

This handbook supports key ISO 27001 control domains, including:

- A.5 – Information Security Policies
- A.6 – Organization of Information Security
- A.8 – Asset Management

- A.9 – Access Control
 - A.12 – Operations Security
 - A.14 – System Acquisition, Development and Maintenance
 - A.16 – Incident Management
 - A.17 – Business Continuity
-

7.3.2 SOC 2 Alignment

This handbook supports SOC 2 Trust Service Criteria:

- Security – Protection against unauthorized access
 - Availability – System uptime and resilience
 - Confidentiality – Protection of sensitive data
 - Processing Integrity – Accurate system processing
-

7.3.3 Regulatory Considerations

This handbook is aligned with industry best practices and frameworks such as:

- Data protection regulations (e.g., GDPR)
 - Industry security best practices
 - Internal governance requirements
-

7.3.4 Continuous Compliance

To maintain compliance:

- Controls must be continuously monitored
 - Policies must be regularly reviewed
 - Audits must be conducted periodically
 - Improvements must be implemented based on findings
-

Contact Information

For questions, clarifications, or reporting security-related matters, please contact:

Information Security Team

Pegasus19 N.V.

Email: tech@pegasus19nv.com

For incident reporting, refer to the Incident Response Plan (Section 4.1).

Approval

This Information Security Handbook has been reviewed and approved by authorized representatives of the Company

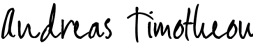
By signing below, management confirms commitment to the implementation and enforcement of the policies contained in this document.

Information Security Manager

Name: Andreas Timotheou

Signature: _____

Date: 5/27/2026

Signed by:

B79D559F46A049E...

Executive Management / Director

Name: Andreas Timotheou

Signature: _____

Date: 5/27/2026

Signed by:

B79D559F46A049E...