

Panbet Curacao NV

Information Security Policy Version 2.7

Confidential

Panbet Curacao NV Information Security Policy

Version History

This document will be distributed to the following people for review:

Version	Date	Summary of Changes	Author
1.0	26/08/2015	New document	Gregory Mishchiy
2.0	22/03/2018	Updated version	Robert Shipway
2.1	27/06/2018	Document Review	Gregory Mishchiy
2.3	24/01/2022	Yearly review	Milen Tenev
2.4	29/05/2023	Yearly review	Milen Tenev
2.5	17/06/2024	Yearly review	Milen Tenev
2.6	13/02/2025	Yearly review	Milen Tenev
2.7	15/04/2025	Major rework	Milen Tenev

Panbet Curacao NV Information Security Policy

Approvers

This document will require approval from the following people:

Name	Position	Organisation	Version
Natalia Zavodnik	Director	Panbet Curacao NV	1.0
Natalia Zavodnik	Director	Panbet Curacao NV	2.0
Natalia Zavodnik	Director	Panbet Curacao NV	2.3
Natalia Zavodnik	Director	Panbet Curacao NV	2.4
Natalia Zavodnik	Director	Panbet Curacao NV	2.5
Gregory Mishchiy	Director	Panbet Curacao NV	2.6
Gregory Mishchiy	Director	Panbet Curacao NV	2.7

Approved by Gregory Mishchiy_____, Date 17.08.2025

Panbet Curacao NV Information Security Policy

Contents

Contents.....	4
Standard – A.5 Organisational Controls	8
Objective A.5.1 Policies for Information Security	8
IT Department	8
Practical Arrangements	9
Equipment Authentication	12
Change Control Procedures	13
Requirement A.5.1.1 Policies for Information Security	14
Requirement A.5.1.2 Review of the policies for information security	14
Objective A.5.2 Information Security Roles and Responsibilities	14
Objective A.5.3 Segregation of Duties.....	14
Objective A.5.4 Management Responsibilities	14
Objective A.5.5 Contact with Authorities	14
Objective A.5.6 Contact with Special Interest Groups	15
Objective A.5.7 Threat Intelligence	15
Objective A.5.8 Information Security in Project Management	15
Objective A.5.9 Inventory of Information and Other Associated Assets.....	15
Objective A.5.10 Acceptable Use of Information and Other Associated Assets	15
Objective A.5.11 Return of Assets	16
Objective A.5.12 Classification of Information	17
Objective A.5.13 Labelling of Information	17
Objective A.5.14 Information Transfer	18
Objective A.5.15 Access Control	18
Physical access policy	18
Remote Access Policy	19
Objective A.5.16 Identity Management.....	20
Panbet Curacao NV internal procedures.....	20
Customer related manufactured software/production/operations	20
Objective A.5.17 Authentication Information	22
Internally	23
Customer Passwords	23
Basic Password Best Practice for Internal Employees.....	26
User Status	27
Changing a Password.....	27

Panbet Curacao NV Information Security Policy

Password Security	27
Setting Up a New User	28
Domain Password Policy	28
OddsCompiler System (back office)	29
Shared Utilities	29
Objective A.5.18 Access Rights	31
Objective A.5.19 Information Security in Supplier Relationships	32
Objective A.5.20 Addressing Information Security Within Supplier Agreements	32
Objective A.5.22 Monitoring, Review and Change Management of Supplier Services	32
General guidelines.....	32
Practical arrangements	32
Objective A.5.23 Information Security for Use of Cloud Services	34
Objective A.5.24 Information Security Incident Management Planning and Preparation ...	34
Objective A.5.25 Assessment and Decision on Information Security Events	34
Objective A.5.26 Response to Information Security Incidents	34
Objective A.5.27 Learning From Information Security Incidents	34
Objective A.5.28 Collection of Evidence	34
Objective A.5.29 Information Security During Disruption	34
Objective A.5.30 ICT Readiness for Business Continuity.....	35
Objective A.5.31 Legal, Statutory, Regulatory and Contractual Requirements	36
Objective A.5.32 Intellectual Property Rights	36
Objective A.5.33 Protection of Records	36
Objective A.5.34 Privacy and Protection of PII	37
Objective A.5.36 Compliance With Policies, Rules and Standards for Information Security	39
Standard – A.6 People Controls	41
Objective A.6.1 Screening	41
Objective A.6.2 Terms and Conditions of Employment	41
Objective A.6.3 Information Security Awareness, Education and training	42
Objective A.6.4 Disciplinary Process	43
Objective A.6.5 Responsibilities After Termination or Change of employment.....	43
Objective A.6.6 Confidentiality or Non-Disclosure agreements.....	43
Objective A.6.7 Remote Working	44
Scope	44
VPN Policy	44
Objective A.6.8 Information Security Event Reporting	46

Panbet Curacao NV Information Security Policy

Standard – A.7 Physical Controls	47
Objective A.7.1 Physical Security Perimeters	47
Objective A.7.2 Physical Entry	47
Objective A.7.3 Securing Offices, Rooms and Facilities	47
Objective A.7.4 Physical Security Monitoring	47
Objective A.7.5 Protecting Against Physical and Environmental Threats	48
Objective A.7.6 Working In Secure Areas	48
Objective A.7.7 Clear Desk and Clear Screen	48
Objective A.7.8 Equipment Siting and Protection	48
Server security	48
Objective A.7.9 Security of Assets Off-Premises	48
Objective A.7.10 Storage Media	49
Objective A.7.12 Cabling Security	49
Objective A.7.14 Secure Disposal or Re-Use of Equipment	49
Standard – A.8 Technological Controls	51
1. Device security:	52
2. Network security:	52
3. Authentication and access:	52
4. Data protection:	52
5. Awareness and training:	54
6. Mobile Device Security:	54
Mobile computing and communications	54
Issuing Policy	54
Bluetooth	55
Personal Use	56
PCD Safety	56
Objective A.8.2 Privileged Access Rights	56
Objective A.8.3 Information Access Restriction	57
Employee User Inactivity Timeout	57
Customer User Inactivity Timeout	57
Objective A.8.4 Access to Source Code	57
Objective A.8.5 Secure Authentication	57
Objective A.8.7 Protection Against Malware	58
Objective A.8.8 Management of Technical Vulnerabilities	59
Objective A.8.9 Configuration Management	59

Panbet Curacao NV Information Security Policy

Objective A.8.10 Information Deletion	60
Objective A.8.11 Data Masking	60
Objective A.8.12 Data Leakage Prevention	60
Objective A.8.13 Information Backup	60
Objective A.8.14 Redundancy of Information Processing Facilities	61
Objective A.8.15 Logging.....	61
Objective A.8.16 Monitoring Activities	62
Objective A.8.17 Clock Synchronization	63
Objective A.8.18 Use of Privileged Utility Programs	63
Objective A.8.19 Installation of Software on Operational Systems.....	64
Objective A.8.20 Networks Security.....	64
Objective A.8.21 Security of Network Services	65
General guidance	65
Objective A.8.22 Segregation of Networks	66
Objective A.8.23 Web filtering.....	66
Objective A.8.24 Use of Cryptography	66
Objective A.8.25 Secure Development Life Cycle	66
Objective A.8.26 Application Security Requirements.....	67
Transaction Security Policy	67
Objective A.8.28 Secure Coding	69
Objective A.8.31 Separation of Development, Test and Production Environments	69
Objective A.8.32 Change Management	71

Standard – A.5 Organisational Controls

Objective A.5.1 Policies for Information Security

Purpose and Ownership

This policy has been created by and for the use of PCNV (“**Panbet Curacao NV**”) and its Members which include directors and board members of Panbet Curacao NV, employees of PCNV, Contractors providing specific services including but not limited to software installation, vendors and agents (the “**Members**”). All of this policy can be freely used by the Members.

A security policy provides the impetus for the company to integrate their efforts from the perspective of awareness and communication, as well as coordinated response in times of any security breach. By requiring each department to incorporate these security procedures as part of their daily operations ensures that when an incident occurs, swift mitigation and remediation follows.

The purpose of this policy is to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations. Furthermore, to establish general guidelines for software development and maintaining a safe computing environment (both desktop and server) within the company and across all business operations through the use of manufactured software that is controlled, consistent, secure and will protect customer data.

The day to day management of computer usage will be performed by the department managers. They will be responsible for ensuring that all Members will acknowledge and adhere to the information security policies and procedures.

It is the responsibility of the IT Department and CTO to maintain these policies for the Gaming and Development Servers. Policy enforcement will be the responsibility of the department managers.

System operators will be required to keep their account details private, and a rigid structure of roles and permissions will be implemented to prevent unauthorized personnel having access to sensitive customer information.

Department managers will be responsible for enforcing a local security policy applicable to their specific department.

IT Department

The IT department is responsible for supporting and coordinating the day to day operation of the system users as well as providing support and maintenance for the gaming equipment located in the data centre.

The IT department will provide recommendations on the following:

Panbet Curacao NV Information Security Policy

- New Software purchases.
- New Hardware purchases.
- Automation of procedures.
- Access Control issues.
- System monitoring.
- Suspicious or fraudulent use of the company's equipment.

PCNV has developed regulations with regards to purchasing office hardware and computer equipment. These regulations reside on Confluence.

In addition, the IT department will be responsible for:

- Ensuring system operators have correct levels of permission in the system.
- Ensuring all sensitive reports and customer information are adequately safeguarded and disposed of in a proper manner.
- Monitoring and maintaining control over the appropriate use of hardware.
- Maintaining adequate environmental controls.
- Ensuring that the staff are properly trained in their department.
- Enforcing that procedures and policy are followed.
- Maintaining compliance with the PCI DSS requirements.
- To ensure provision of strong passwords and follow other good practices such as locking a workstation if the user is to leave it for a period of time.

Practical Arrangements

a) Acquisition of New Hardware or Software

The acquisition of all hardware, software, and peripherals must be properly justified and must be subjected to internal risk analysis – this is especially important in the case of new hardware for the gaming servers. All acquisitions, implementations and installations will be carried out by the IT department (with the assistance of specific departments where appropriate).

- All risk analysis will be subject to the risk assessment process. The process has been regulated by PCNV Risk Management Plan and Assessment Policy which resides here:
- All acquisitions that will alter system operations are subject to the procedures detailed in the Change Management Process document.
- All departmental systems will be equipped with a standardized set of software packages such as an anti-virus and text editor. It will be the responsibility of the IT department to periodically review the standard software package installations.
- The IT department will be required to keep and maintain an inventory of all hardware and software used in both the gaming system and the Panbet Curacao NV office.

Panbet Curacao NV Information Security Policy

b) Physical Data Security

All development sources and corresponding files should be stored and processed. Tested data relating to software manufacturing should be stored securely. The same applies to all versions of released builds.

The data centre network setup, access and data storage and other points addressed in the ISO27001 requirements should be managed and reviewed periodically by the IT department. Any proposed change in the systems will require a review of the changes against the mentioned standards. This will be carried out by the IT Department and the Head of Compliance.

It is the responsibility of the Network Manager to ensure that there is adequate physical security and protection of the system hardware and data.

c) Virus and malware Protection

Servers and network equipment at the datacentres is protected from malware, malicious code and viruses by the following means:

- Firewall settings at server operation systems levels (Linux iptables)
- Disabling unnecessary services
- On network equipment – by access lists and by enabling Cisco Intrusion Prevention System protection

Office computers are is protected from malware, malicious code and viruses by the following means:

- Corporate protection has been provided by Kaspersky Antivirus and SentinelOne MDR
- Corporate network perimeter protection on the network equipment (access lists and Cisco IPS where applicable)
- Antispam and Antiphishing protection on the mail servers is provided by Kaspersky Mail Gateway and Office 365 for Microsoft Exchange

d) Access

Access to the development/testing areas will be restricted to authorized Members and contractors only. Remote access to all aspects of the system operation, including remote access to the trading offices and gaming servers will be controlled and monitored by the IT Department. Access to the trading office networks will be performed via a Virtual Private Network. All connections will be logged and reviewed periodically for any abnormalities.

e) Data Cleansing

Panbet Curacao NV Information Security Policy

To ensure that sensitive data does not remain on a storage medium after its lifetime has expired, a number of steps must be taken to eliminate any traces of data. These steps are covered in the PCNV Data Retention Policy. The Policy resides here:
<https://cfl.mara.local/display/GPP/Panbet+Curacao+NV>

f) Backup Planning and Disaster Recovery

More specific details regarding disaster recovery can be located in the Incident Response [Disaster Recovery Policy](#) and [Backup Policy](#) documents. The IT department is responsible for identifying, managing and testing the proper procedures to ensure that hardware, software and documentation is adequately backed up to ensure timely recovery in the event of a disaster.

g) User Support and Training Guidelines

It is important to understand that due to the nature of the Panbet Curacao NV operation, correct usage of a personal computer is very important. All operators and staff should be trained on the system and familiarized with the various policies across a number of areas.

The company will provide operators with computer training on the usage of both the hardware and software aspects. All Members will be educated in general company policies and procedures, with specific policy and procedural training given by a specific department. Providing adequate training will increase a Members' awareness towards computer security risks and vulnerabilities, along with appropriate preventative controls. All training documentation will be reviewed by department managers and the Head of Compliance on a regular basis.

What is more all employees undergo a number of trainings at their start of employment and annually. The trainings include anti-phishing, anti-money laundering, responsible gambling and others. An overview of the training materials can be found here:

<https://cfl.mara.local/display/LANDD/REFRESHER+TRAINING>

<https://cfl.mara.local/display/GPP/Trainings>

h) Policy Awareness

This Policy applies to the directors and board members of Panbet Curacao NV, employees of PCNV, Contractors providing services including but not limited to software installation, vendors and agents (the “**Members**”). Compliance with the Policy will form part of the contractual agreements.

Failure to comply with the Security Policy could negatively impact the ability of the

Panbet Curacao NV Information Security Policy

company to achieve its aims and security objectives and could damage the professional reputation of the organisation.

Failure to comply could result in disciplinary action for the individual in breach.

Panbet Curacao NV will encourage third parties, engaging in joint ventures, to adopt and use this Security Policy.

i) Escalation of Security Breaches

Department Managers will have overall responsibility for information security within their own departments. Overall system information security will be the responsibility of the IT Department.

In the event a security incident is reported, it should be escalated to the appropriate department head where action can be taken to resolve the issue. Depending on the severity of the issue, it should then be recorded formally as a security breach and the security policy will be subject to review immediately following such an incident. The process has been regulated by PCNV Risk Management Plan and Assessment Policy which resides here:

<https://cfl.mara.local/display/GPP/Panbet+Curacao+NV>

j) Enforcement

Any Member found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Equipment Authentication

Unix Server Authentication

Authentication on all servers is done using a physical Yubikey device plugged into the employee's personal computer. In order to access production environment through SSH or to access windows production environment in any interactive way (RDP, remoteapp, etc.), employees must use their Yubikeys as authentication method. These are received upon employment (with "New Starter" Jira task in SD project) or upon request from line manager (with task in SD project). For contractors, yubikeys are purchased by the contractor and are compensated in invoice, for other employees yubikeys are received from IT support directly or via mail. Access is restricted to a small number of users, with each successful and unsuccessful authentication being logged in the /var/log/secure file. Other events such as the issuing of super user rights, password changes, group changes are also logged here. Furthermore, a Wazuh SIEM system is employed as well, described underneath. More information with regards to Yubikey usage can be found here:

<https://cfl.mara.local/display/GPP/Yubikey>

Panbet Curacao NV Information Security Policy

Cisco Equipment Authentication

Authentication for all Cisco network equipment before access to the Cisco IOS command line is done via TACACS+. Each user's login, password and access rights are stored in LDAP/FreeIPA and have been hashed using sha512.

Access to Internal Resources via VPN

VPN authentication is performed using the RADIUS server. In the event of the RADIUS server being inaccessible, the Cisco ASA local RADIUS settings are used. In the event of successful authentication, the user is given an Internet Protocol ("IP") address from the IP pool reserved for VPN connections, and access-list spltt standard permit dc_int 255.255.255.0 is applied to the encrypted connection.

Change Control Procedures

The implementation of changes must be strictly controlled by the use of formal change control procedures to minimize the risk of system corruption. These formalized change controls must be enforced. They should ensure that security and control procedures are not compromised, programmers are given access to only those units required for their work and that formal approvals are obtained. Changing application software can impact the operational environment. Whenever practical, application and operational change procedures should be integrated. These processes should include:

- maintaining a record of agreed authorization levels;
- ensuring changes are submitted by authorized personnel;
- reviewing controls and procedures to ensure they will not be compromised by the changes submitted;
- identifying all the software, databases and hardware that require change;
- obtaining formal approval before work commences;
- ensuring the changes are carried out to minimize any possible disruptions;
- ensuring the system documentation is current;
- maintaining version control on all updates;
- maintaining an audit trail of all change requests; and
- ensuring that operational documentation and user procedures reflect the new environment, and ensuring that the changes are implemented without business disruption.

The process has been regulated by PCNV policy. Is called Panbet Curacao NV Change Management Policy and resides here:

<https://cfl.mara.local/display/GPP/Panbet+Curacao+NV>

Panbet Curacao NV Information Security Policy

Requirement A.5.1.1 Policies for Information Security

An information security policy document shall be approved by management, published and communicated to all Members and relevant external parties. This document is the Panbet Curacao NV Staff Security Policy.

Requirement A.5.1.2 Review of the policies for information security

The Information security policy document will be subject to yearly reviews by the Deputy of The Head of Technical Compliance to take into account feasibility or immediately in the event of a security breach.

Objective A.5.2 Information Security Roles and Responsibilities

All information security responsibilities shall be clearly defined. Management shall actively support security within the organisation through clear direction, commitment, explicit assignment and acknowledgment of information security responsibilities.

Responsible Department	Subject of responsibility	Roles
Technical Compliance	Evaluation of security controls and technologies, assisting with new security projects.	Deputy of The Head of Technical Compliance, Technical Compliance specialist, Security Specialist
ITSEC	Implementation of new security projects	Security Specialist
IS	Implementation of new security projects	Security Specialist

Objective A.5.3 Segregation of Duties

Information security activities shall be coordinated by representatives from different parts of the organisation with relevant roles and job functions. All roles are segregated where possible in a way that personnel can access and work on need to know/do basis. To further enhance this, security functions are segregated between the three Information Security related departments – Technical Compliance, ITSEC and IS.

Objective A.5.4 Management Responsibilities

This policy as well as all other policies and procedures which are forming the Panbet Curacao NV ISMS pack is governed by the CEO\CISO\CCO role as well as the Deputy of The Head of Technical Compliance role.

Objective A.5.5 Contact with Authorities

Appropriate contacts with relevant authorities shall be maintained. Compliance and Legal departments are responsible for contacting any authorities.

Panbet Curacao NV Information Security Policy

Objective A.5.6 Contact with Special Interest Groups

A management authorisation process for new information processing facilities shall be defined and implemented. Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.

Objective A.5.7 Threat Intelligence

Currently the Threat Intelligence is handled by ITSEC and Compliance departments which are using technologies provided by SentinelOne, Kaspersky, Alienvault OTX, Wazuh and MITRE as well as other industry approved sources.

Objective A.5.8 Information Security in Project Management

All projects are a subject of Information Security review performed by either or all of the three main Information Security departments. This is done through a Jira task in their relevant Jira spaces – CMPL, ITSEC, IS.

Objective A.5.9 Inventory of Information and Other Associated Assets

All information and other assets are maintained in their relevant Confluence pages.

Objective A.5.10 Acceptable Use of Information and Other Associated Assets

Procedures for the handling and storage of information shall be established in order to protect information from unauthorised disclosure or misuse. Information should be labelled and handled consistently in accordance with its classification irrespective of the media contained.

All information held should be classified according to the following definitions:

- **Unclassified Public.** Information that is not confidential and can be made public knowledge without any implications for Panbet Curacao NV. Loss of availability due to system downtime is an acceptable risk. Integrity is important but not vital.
This class of information has to be backed up according to the general procedures; however no encryption or any other means of special protection are required. No access restrictions.
- **Proprietary.** Information is restricted to management approved internal access and protected from external access. Unauthorized access could influence Panbet Curacao NV. operational effectiveness, cause an important financial loss, provide a significant gain to a competitor or cause a major drop in customer confidence. Information integrity is vital. Software source codes and compiled codes are part of proprietary information.
This class of information has to be backed up according to the general procedures; however no encryption or any other means of special protection are

Panbet Curacao NV Information Security Policy

required. Access to this information shall be provided only for approved users and only via company networks and/or VPN.

- **Client Confidential Data.** Information received from clients in any form for processing in production by Panbet Curacao NV. The original copy of such information must not be changed in any way without written permission from the client. The highest possible levels of integrity, confidentiality and restricted availability are vital.

This class of information shall be encrypted and backed up by methods determined by this Policy. Access shall be granted only to authorised users via company networks and/or VPN.

- **Company Confidential Data.** Includes algorithms, passwords and encryptions keys required for information exchange within the company, customers and third party services. Also customers data (personal data and transactions data), transaction logs on the production system and information collected and used by Panbet Curacao NV in the conduct of its business to employ people, to log and fulfil client orders and to manage all aspects of corporate finance. Access to this information is very restricted within the company. The highest possible levels of integrity, confidentiality and restricted availability are vital.

Please see the Group [Data Classification Register](#) for further guidance on the handling of information in accordance with the above classifications. This class of information shall be encrypted and backed up by methods determined by this Policy. Access shall be granted only to authorised users via company networks and/or VPN. From the point of view of physical security this information shall be stored in approved data centres only that are ISO 27001 certified.

PCNV has developed a Data Protection Policy which is to be updated regularly. It defines what personal data is, data protection principles, procedure for accessing employee's personal data, and how to make a complaint. The policy can be reviewed by accessing the following link:

<https://cfl.mara.local/display/BRHR/Data+Protection+Policy>

<https://cfl.mara.local/pages/viewpage.action?pageId=348423689>

Objective A.5.11 Return of Assets

The return of company owned assets is handled by the relevant Heads of Departments and/or Team Leads and the process is owned by the relevant IT departments in all Group Entities. When a new ticket is received from HR that person is leaving or dismissed, IT team should:

Collect all equipment issued to the employee and complete the IT Equipment Return Form

<https://cfl.mara.local/display/TEC/Leaver+Process>

Objective A.5.12 Classification of Information

All Group Entities information is classified according to the [Data Classification Register](#).

Individual classifications can be assigned based on individual Entity or Department needs.

Objective A.5.13 Labelling of Information

All employees are mandated to label the information that they share with third parties when it's classified as confidential. The labelling shall be done in a clear way for the recipient of information, for example, marking emails as confidential, adding CONFIDENTIAL suffix/prefix to the file name, adding CONFIDENTIAL to the beginning of an email message, commenting in Jira, Confluence or in chat groups and etc.

Training slides:

Confidential information

Confidential information includes:

- the personal data of customers and employees
- internal information about the company
- corporate IT system details
- internal documents
- any information stored on company databases or backup copies of such data, regardless of how old they are.

The slide features a central graphic of a laptop with a shield icon on its screen, surrounded by icons representing a person, a document, a gear, and a folder.

Confidential information

ANY INFORMATION THAT COMES FROM THE COMPANY'S IT SYSTEM SHOULD BE TREATED AS CONFIDENTIAL.

COMPANY INFORMATION MUST ONLY BE STORED ON COMPANY DEVICES!

YOU MUST NOT FORWARD ANY COMPANY INFORMATION TO, OR STORE ANY COMPANY INFORMATION ON, ANY PERSONAL DEVICE!

Panbet Curacao NV Information Security Policy

Objective A.5.14 Information Transfer

All information in transit to be sent outside of the Panbet Curacao NV must be transferred securely in an encrypted way, for example by using TLS encryption or in password protected archive file or in any other equivalent way. In case when an employ needs help they shall contact ITSEC or Compliance through the established channels like Jira tasks in CMPL/ITSEC spaces or through the company approved chat software Marik.

Objective A.5.15 Access Control

Physical access policy

The purpose of having a physical access policy is to ensure that no unauthorized individual is given access to the sites that are used for production. Limited access to the site will eliminate the risk of malicious actions being taken on the physical servers and also allow traceability if an error occurs.

The company policies allow admission to the development/testing areas and CLC to a certain list of Members.

Physical intrusion detection must be in place to notify of any unauthorized access to the site. In the event the data centre has been entered without the proper procedure of access control being used, it shall be considered an intrusion and the appropriate measures must be taken in order to control the breach according to the ISO 27001 Standard and the datacenter own policies and procedures.

The access restrictions will protect all network jacks that are publicly accessible. Currently, there are no wireless network devices that connect to servers.

Only designated key-personnel have physical access to the development/testing areas and data-centres hosting the production environment. The list is divided in two levels of access:

- Physical: These individuals have the authorization to enter development/testing areas and the data-centre.
- Designated: These individuals have the authorization to enter development/testing areas and the datacentre and also change the list of personnel who are authorized physical access. Designated individuals are;
 - CTO
 - CEO

In order for a visitor to be granted access, they must be identified with official identification to ensure that he has the correct authorization. When such visitors have been allowed entry into the site, the visitor is assigned a visitor's badge to be able to be

Panbet Curacao NV Information Security Policy

identified by other employees. In no circumstances will the visitor be allowed to be present without a visitor's badge. Panbet Curacao NV does not allow external visitors besides the pre-approved cleaning personel, official fire department representatives and Health and Safety officials.

All visits that have followed the proper process shall be logged. The logging will record the names of the persons that have visited the data centre and the time at which they visited. The logs must be retained for at least three months.

PCNV has developed a specific Policy for Whiteroom environments. It resides here:

<https://cfl.mara.local/display/ISHR/White+Room++Environment+Policy>

<https://cfl.mara.local/display/BRHR/White+Room++Environment+Policy>

Furthermore, PCNV has specific Video Surveillance Policies: They reside here:

<https://cfl.mara.local/display/ISHR/Video+Surveillance+Policy>

<https://cfl.mara.local/display/BRHR/CCTV+Policy>

Remote Access Policy

This policy applies to all Members with a Panbet Curacao NV-owned or personally-owned device used to connect to the Panbet Curacao NV network. This policy applies to remote access connections used to carry out work on behalf of Panbet Curacao NV, including reading or sending email and viewing intranet web resources

Remote access implementations that are covered by this policy include VPN + 2FA and SSH. Further information reside here:

<https://cfl.mara.local/pages/viewpage.action?pagelId=399725424>

Details:

- a) Operating System configuration should be in accordance with approved InfoSec guidelines. Further information can be found here:
<https://cfl.mara.local/pages/viewpage.action?pagelId=165071991>
<https://cfl.mara.local/pages/viewpage.action?pagelId=359290505>
- b) Services and applications that will not be used must be disabled where practical.
- c) Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.
- d) The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- e) Trust relationships between systems are a security risk and their use should be avoided. Do not use a trust a relationship where another method of communication is available.
- f) Always use standard security principles of least required access to perform a function.
- g) Do not use root or administrative when a non-privileged account is available.

Panbet Curacao NV Information Security Policy

- h) Privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec and HTTPs) and using physical security keys - yubikeys. Procedures relating to usage of yubikeys can be found in the Yubikey Policy.
- i) All servers should be physically located in an access-controlled environment, with access granted to a restricted number of Members.
- j) Servers are specifically prohibited from operating from uncontrolled cubicle areas.

Remote access security policy

- It is the responsibility of Members with remote access privileges to Panbet Curacao NV's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Panbet Curacao NV.
- Remote Access must only be made by the Member. Members must ensure that their computers are not accessible to others. They must not create any other user accounts on their computer for other people. They must lock/turn off their computer at all times whilst they are away from it. The Member bears responsibility for the consequences should their access be misused.
- To gain remote access to the internal network, a Member will be required to create a task in SD project (<https://jira.mara.local/projects/SD>) with access request and request of appropriate management approval. To provide remote access to new Members (new starters in company) this shall be done by HR employee in advance. This will then have to be approved before the IT department can make any changes. Please see the information below for more details.

Objective A.5.16 Identity Management

Panbet Curacao NV internal procedures

Each manager can initiate a request to extend/grant access permissions for personnel in their team. The manager forwards the request to create user IDs with access rights to the service desk, which results in access on a need-to-know basis accordance with internal procedures. The issuance of access permissions may require an approval from the information security department in accordance with the procedures. User IDs and access permissions should be reviewed quarterly, and any access permissions that are no longer needed will be removed.

Customer related manufactured software/production/operations

The registration process requires the customer to confirm that they agree with the company's Terms and Conditions and Privacy Policy before the registration can be completed. Failure to tick the T&C/Privacy Policy check box and thus not agreeing to these key conditions will result in the customer not being able to complete their regis-

Panbet Curacao NV Information Security Policy

tration. The terms & conditions are found in the General Rules area of the 'Help' section on the website.

The customer registration process is guided and contains all security controls necessary like mandatory fields, input data validation and etc. A customer registration can be made using the system only if certain conditions are met, these include:

- The customer has agreed to the bookmaker's terms and conditions;
- The customer is over the minimum age limit (i.e. Over 18);
- During the registration process a unique user name is entered;
- During the registration, the customer doesn't enter a previously used name and address combination;
- Other combinations, such as matching surname and postcode, will send an alert to the system. The Fraud Department will check these alerts to ensure that the new account is not a duplicate (possibly including the involvement of the Trading department);
- The customer provides a valid email address.

The registration process starts when the customer presses the 'Join Now' button which is located on the top menu of the website. The registration process is entirely automated ensured by data input validation fields that are also mandatory for the creation of a new account. The Jurisdiction Risk Database is reviewed monthly by the Panbet Curacao NV Compliance Officer.

A brief description of the process is given in the following paragraphs:

Personal Details

During the first stage the customer must enter their personal details, with the following fields being mandatory:

- Title
- First name
- Surname
- Date of Birth
- Post Code
- Country
- Address Line 1
- City/Town
- Email address
- Confirm Email address
- Phone number

Because under age gambling is prohibited, the customer cannot enter a date of birth less than the current date minus 18 years.

Panbet Curacao NV Information Security Policy

Account Details

The customer will need to enter details for their online account such as the user name and password. The following information is mandatory:

- Password
- Confirm password
- Currency
- Odds Type
- Customer Services Secret Question and Answer
- Confirmation that the user agrees to the privacy policy, cookie policy has read the terms and conditions and is over 18 years of age.

Once all of the mandatory account details have been completed for steps one and two, the customer has agreed to the company's terms and conditions and confirmed that they are over 18 years of age, the customer can press the 'join now' button to create an account in the system. Once a customer has registered their account they will only be able to commence wagering once they have made an initial deposit. Any free bet offers, which the company may provide will only be activated after the customer's first bet has been settled and their account details have been verified. This will be detailed in the terms and conditions relating to Bonuses and Offers in the 'Help' section on the website. There will be no free bet offers or introductory offers allowing anyone to place a bet without them having made an initial deposit first. After a user has registered their details an account will be opened providing it passes all the checks, described in below. An online customer will be sent an email confirming their registration. When a player 'logs-on' to the website, they have to enter a combination of a unique email address and password. Likewise, when a user makes a telephone call to the Customer Care Team, they have to quote their email address.

A number of alerts are generated for the support centre staff when customers attempt registration with existing data or attempts to change their account details. These alerts are accessible to all system operators with relevant permissions.

The generated alerts include:

- Duplicate Details (e.g. name, email address, telephone number);
- Duplicate address.

Objective A.5.17 Authentication Information

Each user will have his/her own password to access his/her computer in addition to an individual password to start department specific programs, such as in Operations or Finance. Only the System Administrator will have the main passwords and the ability to add or remove users to the system.

The allocation of passwords shall be controlled through a formal management process.

Panbet Curacao NV Information Security Policy

Internally

Secure access by the Members must be strictly controlled via an account identifier/password pair authentication prior to being permitted to access the system. The Panbet Curacao NV system limits the number of failed logon attempts to 5. After five failed logon attempts the account will be locked.

At no time should any Member provide their login password to anyone. Members SHALL NOT:

- Share passwords with anyone, including family members, administrative assistants or secretaries;
- Write passwords down or store them on-line.

All passwords are to be treated as sensitive confidential information. If an account or password is suspected to have been compromised then Members are required to report the matter to the IT Security who will escalate to the CEO when necessary.

Members should choose a strong password, having the following characteristics:

- Contain at least twelve alphanumeric characters long;
- Should be comprised of letters, numbers and special characters;
- Should not be based on any personal information; and
- To use password best practice as described below.

The company's system must use a password history log to maintain a password history of users. The history file should contain the last 24 passwords of users and store them in encrypted form.

Passwords on the system should be changed every 3 months. Every user will be prompted to change his password and will be advised of this five days before the password expiration.

Customer Passwords

The gaming software developed by Panbet Curacao NV has to ensure that customer passwords are never made visible to anyone else other than the customer themselves – such as system operators in the customer support centre. Passwords are not sent in an unencrypted format, but rather as a link to a page where a customer can enter new password details. Furthermore, this link will expire after it has been used to recover a password once. Additional security is provided by ensuring that password recovery steps will only ever be sent to a customer's registered email address. PCNV has implemented new hashing algorithm Argon2id.

1. Strong password requirements:

Minimum length: Require passwords of at least 12 characters.

Complexity: Forcing the combination of upper and lower case letters, numbers, and symbols.

Panbet Curacao NV Information Security Policy

Prohibition of personal information: Avoid the use of names, dates of birth or common words.

Uniqueness: Recommend not reusing passwords on different platforms.

2. Password Management Policies:

Expiration: Set an expiration period for passwords and force their periodic change.

Account lockout: Implement an account lockout system after several failed login attempts.

Password history: Prevent reuse of previous passwords.

3. Fraud monitoring and detection:

Suspicious login attempt detection: Monitor login attempts from unusual locations or devices.

Behavioral Analysis: Use behavioral analysis tools to detect fraudulent activity.

Security Alerts: Generate automatic alerts for suspicious activity.

4. Secure password recovery:

Robust security questions: Use security questions that are difficult to guess and are not readily available online.

Email or SMS verification: Send verification codes to registered email addresses or phone numbers.

Secure recovery process: Ensuring that the password recovery process is secure and prevents unauthorized access.

Recovery from the Website

1. Password recovery from the website is initiated by clicking the forgotten/lost password link. The customer is then taken to the password recovery page where they will be required to enter their username and date of birth. Once this has been entered, the customer will need to press the 'Next' button;
2. This will send the username and date of birth data to the server, where a check will be made for their validity. If entered incorrectly, a message will be displayed. On the third incorrect attempt the user will be redirected to the home page;

Panbet Curacao NV Information Security Policy

3. If the username and date of birth match, an email is sent to the customer's registered email account with a link to the new password page. As soon as the email is sent, the existing password hash is dropped from the database, meaning that the user will not be able to use their old password in the event if they remember it. Once the user follows this link, they will be able to enter a new password and to confirm it a second time. As an additional security feature, the user will be required to enter their username before they set the new password;
4. Once a customer's password has been restored from the link, the link becomes inactive and cannot be used again.

Recovery from the Customer Support Centre

1. Password recovery from the customer support centre follows a similar pattern as the website. A customer will call in, request a password reset, and subject to customer identification procedures, the operator will then decide whether to use the recover password button.
2. When the 'recover password' button has been selected, the password recovery process is generated – i.e. an email is sent to the customer's registered email account with a link to the new password page. As soon as the email is sent, the existing password hash is dropped from the database, meaning that the user will not be able to use their old password in the event if they remember it. Once the user follows this link, they will be able to enter a new password and its confirmation. As an additional security feature, the user will be required to enter their username before they set the new password.
3. Once a customer's password has been restored from the link, the link becomes inactive and cannot be used again.

Sending the Password Link to a Changed Email Address

1. The new password can only be sent by email. The operator cannot see an existing web password or set a new one themselves. If the customer wants the reset password link sent to their current email address then they will be asked their username, full name and CCSQ answer. In the case of webchat correspondence, the customer will be required to complete these details in a pre-chat pop-up.
2. If the customer requests to change their email address first (if their current one is no longer active etc.) then in addition to the questions asked above they will also be required to provide full identification documentation to verify their identity (one document as proof of age and identity, and another as proof of address).

Panbet Curacao NV Information Security Policy

3. Once these questions have been answered correctly then the link to change their password will be sent to the new email address. From this link the customer will still be required to enter their username before being able to enter a new password

Basic Password Best Practice for Internal Employees

Do Not Share Passwords!

Do not share your password with ANYONE – not friends, co-workers or family members.

Your password is the only thing that ensures privacy of your account. It is also your obligation to see that only you use your account. You are responsible for how your account is used, so do not let other people have access to it. Any actions taken by an operator after having logged in using the correct username and password will be attributed to that user.

Make it Hard to Guess!

When creating your password do not use anything that would be easy for someone to guess. For example, never use any part of your user name or legal name. Do not use your phone number, birth date or license plate number. Do not use any popular password combinations as part of your password (qwerty, 123456, admin, user, password, password01 etc.)

Additionally, a longer password equals better security. The longer your password is the harder it is for someone to figure out.

The password must be at least 12 characters long and contain a mix of numbers and letters.

But Most Importantly... Keep your password hidden.

Do not write your password down on a piece of paper. Instead commit it to memory! Never put your password on sticky notes on your monitor or desk.

Passwords will be changed every 90 days and cannot be a repeat of any of your previous 24 passwords. Failure to change your password at this time will result in your account being locked out and the System Administrator will have to reinstate your account on entry of a new password.

Forgotten Password

If a user incorrectly enters their password 5 times the system will lock their user account. Their account can then only be reinstated by the System Administrator and the user will have to enter a new password.

Panbet Curacao NV Information Security Policy

Encryption

All passwords are encrypted and rendered unreadable during entry and storage in all areas.

Password Procedures (Odds Compiler)

The Network Manager/ System Administrator will be responsible for overseeing the setting up of new user accounts and ensuring that passwords are changed as necessary at the correct times.

User Status

Each user will be assigned a status by the Network Manager System Administrator. These will be Active (for current Members), Suspended (for Members undergoing any investigation and/or disciplinary hearings) and Closed (for Members who no longer work for the company).

Changing a Password

If a password is expiring or the user wishes to change a password they can do this themselves once they have logged in. If a password has expired and they are not able to log in then the Network Manager/System Administrator will be able to access their User Page and allow a new password to be set.

Password Security

If you suspect that anyone might be aware of your password, or it has been compromised in any way, then the Network Manager/System Administrator must be made aware IMMEDIATELY. They will disable the account and ask the user to set a new password. The user will be required to check the log in history at the same time and must make the System Administrator/Network Manager is informed immediately should there be any logins or actions which the user does not recall being made by them. Every user will have their own username and password. No shared or group accounts and passwords are allowed.

Member Leaving

If a Member leaves the company their user account must be disabled on leaving or earlier if appropriate. The user account is kept in the system for future audit and security purposes, but the user account will be set to closed. In this state no one will be able to access that account as a user. HR will inform the manager and IT department of any leavers. Any user ssh keys or active directory certificates must be deleted, and their yubikey (if they had one) must be reset.

Panbet Curacao NV Information Security Policy

Member Suspension

If a Member is suspended during the course of their employment pending any investigations then their user account will immediately be set to suspended. In this state the user will not have any access to the system. The suspension duration shall match the timeframe of the temporary suspension/disablement of the system accounts.

Setting Up a New User

Users within the Panserve Domain

Each user will be allocated a username and will set their password. However, the first (initial password) is set from IT Technician and is communicated securely to the user. Securely communicated is considered to be sending the username in on channel like email and the password in an approved messenger application like Marik where the descriptive text shall be in the email while nothing than the password shall be in Marik. Or alternatively both username and password can be sent as a password encrypted attachment (archive) in an email + the password for the archive shall be sent in Marik, where all passwords shall be generated in a strong way as per this policy. Passwords that needs to be sent to external parties must be sent only as an encrypted attachment by email where the password shall be sent to the recipient by SMS message to their personal or company owned mobile phone. The initial password can't be used for login and any other activities than setting a personalized password from the user itself. The initial password is always unique and follows the Domain password policy. Some computers, for example Customer Service Operatives and Traders, will be shared –therefore, it is essential that the password details remain secure. The user must ensure their password is not divulged to anyone else and that when entering it, either initially or at login, that no one can see it being typed. Before the user has entered a password they will not be able to access their user account. User accounts will be subject to a time out – after a user has been inactive for 5 minutes, their computer is locked automatically. Upon return, they will need to re-enter their password in order to log back in.

Domain Password Policy

It is company policy for all computers connected to the PANBET domain to have a number of security features with regards to passwords. These are:

- All passwords will expire after 90 days
- A user will not be able to enter a new password that is the same as their 24 previous passwords.
- A user domain account will be suspended if their password is entered incorrectly 5 times.
- Passwords must be strong and comprise of at least 8 characters – made up of a combination of numbers and letters and a symbol.

Active Directory Password requirements:

Panbet Curacao NV Information Security Policy

Length: 12 Characters

Complexity: Enabled. Passwords must contain characters from three of the following five categories: Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters); Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters); Base 10 digits (0 through 9); Nonalphanumeric characters: ~!@#\$\$%^&* - +='\(){}[]:;'"<>.,.?/; Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian language.

Password History: 24

Maximum Password age: 90 days

Minimum password Age: 1 day

Can't include: user's name, surname, login name or part of user's name, surname, login name

[OddsCompiler System \(back office\)](#)

The user will be allocated a username and be required to enter their unique password.

[Shared Utilities](#)

There will be a shared file management programme for files which need to be accessed by more than one person. This will allow communal files to be accessed by more than one person without compromising anyone's login details.

Remote Access

Procedures relating to remote access passwords can be found in the Remote Access Policy. The general password best practice guidelines apply across all passwords in all parts of the system and by all users. A list of all users with remote access can be found in the Remote Access Register.

Remote Access Root User Passwords

Passwords for all emergency root, administrator or super user will be stored securely in a safe. These passwords will be maintained and kept safe by a senior manager but not by the IT Department manager.

These passwords will be made available to system administrators on request to ensure that one person does not hold all the keys. A new service has been employed called Vault by HashiCorp. It stores credentials, tokens, passwords and secret URLs. All data is stored in an encrypted container. It request to Vault is logged for future

Panbet Curacao NV Information Security Policy

auditing. Vault supports the full secret lifecycle – creation, revocation, expiration and renewal. PCNV has employed 8 clusters. Further information can be found here: <https://cfl.mara.local/display/PIR/Vault+by+HashiCorp>

Actual password creation for administrator, root or super user passwords must follow the best practice guidelines specified in this document.

Systems for managing passwords shall be interactive and shall ensure quality passwords.

The Network Manager/System Administrator will be responsible for overseeing the setting up of new user accounts and ensuring that passwords are changed as necessary at the correct times.

Each user will be assigned a status by the Network Manager/System Administrator. These will be **Active** (for current Members), **Suspended** (for Members undergoing any investigation and/or disciplinary hearings) and **Closed** (for Members who have left the company).

If a password is about to expire or the user wishes to change a password they can do this themselves once they have logged in.

If a password has expired and they are not able to log in then the Network Manager/System Administrator will be able to access their User Page and allow a new password to be set.

If you suspect that anyone might be aware of your password, or it has been compromised in any way, then the Network Manager/System Administrator must be made aware IMMEDIATELY. They will disable the account and ask the user to set a new password. The user will be required to check the log in history at the same time and must make the System Administrator/Network Manager aware instantly should there be any logins or actions which the user does not recall being made by them. Every user will have an individual username and password. No shared or group accounts and passwords are allowed.

If a Member leaves the company their user account must be disabled on leaving, or earlier if appropriate. The user account is kept in the system for future audit and security purposes, but the user account will be set to closed. In this mode no one will be able to log into that account as a user.

Setting Up a New User

Each user will be allocated a username and will set their password. Some computers, for example Customer Service Operatives and Traders, will be shared so it is essential that the password details remain secure. The user must ensure their password is not divulged to anyone else and that when entering it, either initially or at login, that no one is able to see it being typed. Before the user has entered a password they

Panbet Curacao NV Information Security Policy

will not be able to access their user account. User accounts will be subject to a time out – after a user has been inactive for 5 minutes, their computer is locked automatically. Upon return, they will need to re-enter their password in order to log back in.

It is company policy for all computers connected to the Panbet Curacao NV domain to have a number of security features with regards to passwords. These are:

- All passwords will expire after 90 days.
- A user will not be able to enter a new password that is the same as their 24 previous passwords.
- A user domain account will be suspended if their password is entered incorrectly 5 times.
- Passwords must be strong and comprise of at least 8 characters – made up of a combination of numbers and letters and a symbol.

Objective A.5.18 Access Rights

Each manager can initiate a request to extend/grant access permissions for personnel in their team. The manager forwards the request to create user IDs with access rights to the service desk, which results in access on a need-to-know basis accordance with internal procedures. The issuance of access permissions may require an approval from the information security department or Compliance in accordance with the procedures. User IDs and access permissions should be reviewed quarterly, and any access permissions that are no longer needed will be removed.

- System Authorisation Requests for the deletion of accounts is done according to the Access Control policy.

PCNV has developed a Policy with regards to regulating access control to the Company's information resources. It outlines the whole process, its workflow and employee's duties and responsibilities. Further information is to be found here:

<https://cfl.mara.local/pages/viewpage.action?pageId=184663755>

- HR shall inform the IT department via task in SD Jira project (<https://jira.mara.local/projects/SD>) when they process a termination of a Member and/or a consultant. This is done in advance (as soon as appropriate). Access rights shall be removed on the last day of employment or on termination.
- In addition to the above list of informants the Chief HR Officer shall be informed in case of a dismissal. This is done either by the employee with submitting a notice period of a leave or by the relevant Team Lead/Head of Department.
- HR is handling the processes of termination of contractors.
- Internal IT team shall compare the list from HR with the user accounts databases and performs a purge (clean-up) if necessary. Purged accounts will be recorded as a request for revision - and logging purposes. It is acceptable to put the ac-

Panbet Curacao NV Information Security Policy

counts in disabled/suspended state for audit purposes, re-hires and return from long leave.

Objective A.5.19 Information Security in Supplier Relationships

All third parties and employees to be hired are a subject to a DD process which includes Security related checks performed by the IS department.

Objective A.5.20 Addressing Information Security Within Supplier Agreements

All contracts with third parties must contain Information Security clauses as well as GDPR, NDA and any other relevant clauses.

Objective A.5.22 Monitoring, Review and Change Management of Supplier Services

It is essential security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated and maintained by the third party.

General guidelines

The services, reports and records provided by a third party shall be regularly monitored and reviewed by the Department which is managing/maintaining the service and audits may be carried out regularly by external parties as well as by Compliance/IT/IS/ITSEC when necessary. Additionally Extended Due Diligence is performed by the Executive Support department on any new to the Group Entities suppliers.

Practical arrangements

Feed loader monitoring

The following monitoring mechanisms are in place to ensure the working state of the feed loader:

No Java Application in the process list. The monitoring system, which is built on Zabbix, checks the process list every 60 seconds to ensure that a Java application used by the feed loader is running. If this process is not present in the process list then the feed loader is no longer working. An automatic notification will then be sent to members of the systems administration department.

Logfile timestamp abnormalities. The feed loader automatically writes an entry in its log file at every load cycle. The monitoring system (Zabbix) checks the feed loader log file modified time, and alerts the system administrators if the last log entry time is greater than the current file load cycle.

Panbet Curacao NV Information Security Policy

Nonreceipt of feed files. Zabbix automatically alerts the system administration department when an expected file is not delivered.

Error logs. The feed loader uses an error logging system based on the Log4j framework. This stores all errors in the following file: "%logs%/error.log", where %logs% is the full path to the directory for storing the feed loader log files. The path %logs% is specified in the settings file "%config%/log4j.xml", where %config% is the full path to the directory for feed loader settings files. All system administrators need to check the specified error log file on a regular basis and deal with any discovered errors in accordance with the server recovery procedures on the server running Logstash shipper, which monitors the error log and sends critical errors to Zabbix server.

Email error notifications. For mail notifications Zabbix is used. Zabbix server informs the system administrators of all critical errors. Email addresses of all recipients are specified in the Zabbix database. A description of the error will be made via email, as well as the accompanying system logs. All system administrators on the mailing list are required to check their mail regularly, and react to any discovered errors in accordance with the server recovery procedures.

No new sport events and changes when they are expected. When new data does not enter into the system from the feed loader when it should (for example, placings after a horse race during periods when there is racing), it is a clear indicator that the feed loader does not work. System users (operators) must inform the system maintenance and support team should they detect any error in the data transmission (coming into the system). A description of the error will be available in the feed loader error folder.

The operators will need to inform the system administrators should any error occur within the feed loader data delivery.

Penetration testing and vulnerability scanning

Penetration testing and vulnerability scanning have to be performed at least once a year using reputable tools or external resource with required level of certification.

PCNV has developed a number of policies for Service creation, and Validation of new IT services, adding a new service to the Local Environment and creating new Service passports. They can be reviewed by accessing the following links:

<https://cfl.mara.local/pages/viewpage.action?pageId=408746198>

<https://cfl.mara.local/pages/viewpage.action?pageId=418201908>

<https://cfl.mara.local/pages/viewpage.action?pageId=64038982#tab-ENGLISH+VERSION>

<https://cfl.mara.local/pages/viewpage.action?pageId=223679647>

Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls shall be managed, taking into

Panbet Curacao NV Information Security Policy

account the critical business systems and processes involved and assessment of risks.

Objective A.5.23 Information Security for Use of Cloud Services

Cloud services are usually not permitted within the Panbet Curacao NV unless otherwise specifically evaluated and authorized by ITSEC, IS and Compliance departments within a Jira task.

Objective A.5.24 Information Security Incident Management Planning and Preparation

Panbet Curacao NV has developed a specific Incident Management Policy. It outlines management responsibilities, the responsible parties and stakeholders, defines the risk assessment procedure, the risk measurement classification, the response plan and the staff training. What is more, the policy describes the preventative and corrective actions and how to document the how process.

Objective A.5.25 Assessment and Decision on Information Security Events

All information security events are handled by Security Operations within the Technical Compliance, ITSEC and IS departments within by Security Specialists roles. The Security Specialists are required to evaluate all the events while collaborating for their assessments. When necessary, the Security Specialists roles shall escalate to their Team Leads or Head of Department which can escalate further up to the level of the CEO of the Panbet Curacao NV.

Objective A.5.26 Response to Information Security Incidents

There is a Incident Response Plan defined in Incident Management Policy. It describes what actions are to be taken if an incident with the cardholder data has occurred.

Objective A.5.27 Learning From Information Security Incidents

The Incident Management Policy outlines how the organisation can benefit from and learn from information security incidents. Determining the root causes of non-conformities and evaluating potential corrective actions shall primarily be conducted through the Management Review process.

Objective A.5.28 Collection of Evidence

Security Operations have a SIEM technology in place which is collecting all raw logs from all Panbet Curacao NV systems.

Objective A.5.29 Information Security During Disruption

Panbet Curacao NV has developed a procedure which defines what is to be done in the event of Information Security Incident and how it is to be managed.

Panbet Curacao NV Information Security Policy

During an Information Security Incident related disruption, an Incident Management group is formed by the Top Management of the affected Panbet Curacao NV. All further activities are defined within this group by the Top Management on a case by case basis.

Objective A.5.30 ICT Readiness for Business Continuity

Panbet Curacao NV has developed a policy for Business Continuity Planning and Disaster Recovery. The objective is to ensure that any given IT service is capable of providing value to the customer in the event that normal availability solutions fail. Business continuity management primarily considers those IT assets that support key business processes. Should it be necessary to relocate to an alternative working location, provisions are required for items such as office and personnel accommodations, copies of critical paper records, courier services, and telephone facilities to communicate with customers and third parties. The business continuity management process identifies the required and agreed minimum level of business operation following a service disruption, along with a requirements definition covering systems, facilities, and service requirements. The process then examines the risks and threats to these requirements and develops an IT risk reduction or mitigation program. This program implements mechanisms delivering the continuity requirements necessary to provide the required optimum level of business operation. The whole process has been defined in Business Continuity Planning Disaster Recovery Policy, which resides here:

<https://cfl.mara.local/display/GPP/Panbet+Curacao+NV>

Oracle Data Guard ensures high availability, data protection, and disaster recovery for enterprise data. Oracle Data Guard provides a comprehensive set of services that create, maintain, manage, and monitor one or more standby databases to enable production Oracle databases to survive disasters and data corruption. Oracle Data Guard maintains these standby databases as copies of the production database. Then, if the production database becomes unavailable because of a planned or an unplanned outage, Oracle Data Guard can switch any standby database to the production role, minimizing the downtime associated with the outage. PCNV uses physical standby databases. Physical standby databases provide a transactionally consistent, physically identical copy of the primary database, with on-disk database structures that are identical to the primary database on a block-for-block basis. The database schema, including indexes, are the same. A physical standby database is:

- Kept synchronized with the primary database, through Redo Apply, which recovers the redo data received from the primary database and applies the redo to the physical standby database.
- Can receive and apply redo while it is open for read-only access.
- Can therefore be used concurrently for data protection and reporting.
- Can be used to install eligible one-off patches, patch set updates (PSUs), and critical patch updates (CPUs), in rolling fashion.

Panbet Curacao NV Information Security Policy

The standby DB is a backup of the main primary node both at the software level and at the data level. A daily full backup of the DB is taken from the standby DB.

The integrity of the standby DB is automatically tested by Oracle Data Guard mechanisms during the constant restoration of redo logs. Monitoring and notifications are performed through multiple tools: primarily via Zabbix and Oracle Cloud Control, and additionally by log analysis. Zabbix email alerts are being sent automatically to the DB Administrator's department in case of detected issues, Jira tickets are also automatically created and assigned.

All other critical systems, databases, services and file storages are following the same Deploy processes and node cluster configurations where they're using similar to Oracle's Data Guard technologies or those applicable to the Server OS-es, application services, data storages such as OS clustering, Database replications in real-time, high availability proxy services for applications, high availability for network devices, storages configured in RAID and etc.

Objective A.5.31 Legal, Statutory, Regulatory and Contractual Requirements

This process is handled entirely by the relevant Legal department within the Panbet Curacao NV and is taking in consideration all relevant local legislation and regulatory requirements.

Objective A.5.32 Intellectual Property Rights

All Panbet Curacao NV employees are required to protect the Intellectual Property rights of the Group Companies as well as of any third parties. A list of non-exhaustive list of Intellectual Properties:

- Trademark rights.
- Patents.
- Source code licences.
- Software copyright.
- Document copyright.
- Design rights.

Objective A.5.33 Protection of Records

System documentation shall be protected against unauthorised access. The data is encrypted, there are access rights. There is TLS encryptions as well.

All system documentation has to be stored using team collaboration software Atlassian Confluence. Read/Write access to each different area is to be granted by the IT Department by request from the Manager of the corresponding department depend-

Panbet Curacao NV Information Security Policy

ing on the job role of the individual Member. A “need-to-know” basis is to be applied. There is a predefined regulation on granting access to Confluence. A senior member of the team(manager) is to approve the task. A predefined list of people is to be supplied to the APS team in order to outline the employees who are to have been granted access and its level(read/write). The reglament resides here:

<https://cfl.mara.local/pages/viewpage.action?pageId=159288011#>

Objective A.5.34 Privacy and Protection of PII

Ensure that legal, regulatory, and contractual requirements related to privacy and protection of personal data (also called personal data or PII – Personally Identifiable Information) are identified.

Broadly but not limiting, all members of the group must comply with the following:

However, in the case of Panbet Curacao NV, it has a Privacy and Personal Data Protection policy, which can be consulted at the following link:

1.-Legal basis:

- General Data Protection Regulation (GDPR) – European Union.
- Spanish and local Personal Data Protection Law
- International conventions and treaties on privacy.

2.-Legal and organizational requirements:

A. Identification and classification of personal data

- Classify personal information as a sensitive asset.
- Identify the categories of data: identification, biometric, financial, health, etc.
- Distinguish between personal data and sensitive data according to applicable law.
- Flow of personal data by areas and processes

B. Legal basis for processing

- Ensure that each processing has a valid legal basis:
 - Explicit consent
 - Contractual or legal obligation
 - Legitimate interest, among others

C. Principles of treatment

Ensure that the processing of personal data complies with principles such as:

- Lawfulness, loyalty and transparency
- Purpose limitation

Panbet Curacao NV Information Security Policy

- Data Minimization
- Accuracy
- Limitation of the retention period
- Integrity and confidentiality
- Proactive accountability

D. Rights of Rightholders

Establish procedures to allow the exercise of:

- Right of access, rectification, deletion, opposition
- Right to portability and limitation of processing
- Right to be forgotten and not to be subject to automated decisions

3. Recommended technical and organisational controls

A. Organizational controls

- Appoint a Data Protection Officer (DPO) if legally required.
- Keep a record of processing activities (RAT).
- Define privacy policies, disclosure clauses, and confidentiality agreements.

B. Technical controls

- Encryption of personal data in transit and at rest, using robust algorithms.
- Role-based access control (RBAC), with multi-factor authentication (MFA) for privileged users.
- Secure management of passwords and periodic change policies.
- Network segmentation and traffic monitoring to detect unauthorized access.
- Recording and review of activity logs related to the access and processing of personal data.
- Application of the principle of data minimization in the design of processes and systems (Privacy by Design).
- Pseudonymization and anonymization when possible and appropriate.
- Encrypted backups stored in secure locations, with periodic recovery testing.
- Physical restriction of access to systems that store or process personal data.
- Documented procedures for the management of security incidents that include breach notification.
- Data Protection Impact Assessments (DPIAs) for Contracts with data processors that include security and confidentiality clauses.
- Periodic internal and external audits to verify the effectiveness of the security measures implemented.

4. Verification and compliance

Panbet Curacao NV Information Security Policy

- Carry out data protection impact assessments (DPIA/PIA) on high-risk processing.
- Establish procedures for notification of personal data breaches within legal deadlines (e.g. 72h for GDPR).
- Validate the legitimacy of the international flow of data (e.g. standard contractual clauses, adequacy decisions, etc.).

5. Suggested Mandatory Documentation

- Privacy and data protection policy adapted to each country.
- Register of processing activities (RAT).
- Impact assessments (DPIAs).
- ARCO Protocols for Attention to Rights.
- Consent records.
- Data Processing Agreements.

6. Evidence of compliance

- Valid consent records.
- DPIAs reports carried out.
- Staff training minutes on privacy.
- Internal and external audits.
- Documentation of reported breaches and corrective actions.

Objective A.5.35 Independent Review of Information Security

Panbet Curacao NV's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes to the security implementation occur.

In order to achieve required levels of information security Panbet Curacao NV will commission Test Houses approved by the regulator to undertake security audit inspections during the first year of operation and when internal procedures are sufficient to meet requirements of appropriate regulations in full.

Objective A.5.36 Compliance With Policies, Rules and Standards for Information Security

Panbet Curacao NV ISMS pack is available to all employees with access to Confluence.

Panbet Curacao NV Information Security Policy

The Deputy of The Technical Compliance role is responsible to keep those up to date on information security compliance and conduct periodic reviews highlighting areas for improvement, which are thoroughly documented, stored, and reported.

The Deputy of The Technical Compliance role may take the following actions if issues are discovered, and instances of non-compliance are found:

Determine the underlying cause of non-compliance.

Decide whether corrective action is necessary.

If necessary, implement said corrective action to ensure continued compliance.

Once enacted, assess any corrective actions taken to see if they were effective and identify any areas that need to be improved.

It is imperative that corrective actions are taken in a “timely manner”, ideally by the next review. At the very least, The Deputy of The Technical Compliance role should be able to demonstrate progress if measures aren’t completed before the next review.

Standard – A.6 People Controls

Objective A.6.1 Screening

All Panbet Curacao NV HR procedures are including the following partially or completely based on the local legislations:

- Attestations from both business and personal references.
- The CV should be verified to ensure that the candidate has not omitted any relevant information, and that the information is accurate and truthful. This shall be a shared responsibility between HR and the interviewing employ, where for HR this shall be done for specific technical operations roles like IT senior staff, IT Team Leads and Head of Departments and Team Leads/Head Of Department/Top Management, while the interviewing employ shall handle all cases. To achieve this HR shall compare the CV with the candidate's LinkedIn profile, in specific cases, calls to previous HR Managers/Team Leads/Head of Departments in their most recent previous employment company is acceptable and encouraged when relevant, especially for Top Manager's roles. The interviewing employ shall prepare specific job roles questions and/or tests that shall be completed during the interview in an acceptable timeframe.
- The confirmation of professional, academic, and vocational qualifications.
- Verification of identity through the use of an ID card, passport or driving license issued by a government agency or a public sector organisation.
- Any role deemed suitable for enhanced vetting will undergo criminal record checks or basic DBS checks where applicable.

Objective A.6.2 Terms and Conditions of Employment

All Panbet Curacao NV HR procedures are including the following partially or completely based on the local legislations:

- Individuals who are given access to confidential information should sign confidentiality or nondisclosure agreements before getting access to the information assets. Such can be signed as clauses in the employment contract where applicable.
- A description of legal responsibilities and rights (e.g. copyright laws or data protection laws).
- Responsibilities for the classification of information & management of the organisation's information assets.
- The information assets and other associated assets, information processing facilities and information services handled by the personnel.
- The responsibility for handling information received from interested parties.
- If personnel disregard organisational information security requirements, actions need to be taken and explained what they are.
- In addition, the organisation should ensure that personnel agree to terms & conditions concerning information security.

Panbet Curacao NV Information Security Policy

- Panbet Curacao NV has a <https://cfl.mara.local/display/BRHR/Employee+Screening+Policy> applicably only for Panbet Curacao NV personnel.

Objective A.6.3 Information Security Awareness, Education and training

Each Manager has by default, permission to initiate system authorization requests for the personnel within their team. The Manager will escalate the request to the IT Manager who will grant access on a need to know basis. Remote access rights are to be reviewed once every month and any access right which is considered no longer required will be removed.

Third parties will be provided with remote access in very limited scenarios and such access shall be limited to the areas strictly required for the task the third party is engaged. Remote access to third parties is to be granted by the IT Manager and reviewed on a regular basis.

All Members and subcontractors should follow the following general rules:

- Be fully aware of company security policy;
- Information obtained inappropriately should not be used;
- Any security breach, error or fault in the company's systems must be reported to the manager of the business unit and to the CEO and must not be exploited in any way;
- Any information obtained in virtue of employment with the company shall not be disclosed to any third party or misused, unless explicitly authorised by the CEO (in cases such as an enquiry or an investigation by a regulatory authority);
- Any breach of this policy will be subject to the company's review in conformance with the applicable disciplinary procedures and may give rise to legal action against the Member.

The Security Policy must be read in conjunction with the Incident Response Policy which describes in more detail the sequence of actions that must be taken in the event of an incident.

All Members must go through IT Security training on a yearly basis and upon hire. Trainings are delivered by the training department, the power point is located here:
<https://cfl.mara.local/display/LANDD/IT+SECURITY+ENG>
<https://cfl.mara.local/pages/viewpage.action?pageId=249900299>

Panbet Curacao NV Information Security Policy

All Members must remember that misuse of computer systems (including unauthorised use of information, implanting of Panbet Curacao NV malicious code, interference with computer systems) is a criminal offence.

Managers should ensure that Members and contractors are made aware of and are motivated to comply with their information security obligations. For Panbet Curacao NV a disciplinary process is necessary to handle information security breaches. This process is handled by the established local regulations like “Spanish Worker’s Statute” in Spain and ACAS directions in the UK. The process is not applicable to contractors as their contract is of the service type rather than the employment type, the service contracts shall have the relevant clauses to address any penalties or claims related to not complying with the Information Security Policies.

Objective A.6.4 Disciplinary Process

Panbet Curacao NV have different disciplinary processes handled by the HR departments, including:

- Ensuring that regular training sessions are carried out to keep staff up to date on policy changes.
- Designed disciplinary measures for failure to adhere to information security policies.
- Supply each employee with a copy of the organisation’s disciplinary procedures.
- In similar situations, ensure that disciplinary procedures are followed consistently.

Objective A.6.5 Responsibilities After Termination or Change of employment

Security aspects of a person’s exit from the organization or significant changes of roles should be managed, such as returning corporate information and equipment in their possession, updating their access rights and reminding them of their ongoing obligations under privacy laws and contractual terms. When an employee is to leave the organization, HR must inform their Manager and IT for the end of contract and the consequent actions to be taken.

PCNV has developed a Policy with regards to regulating access control to the Company’s information resources. It outlines the whole process, its workflow and employee’s duties and responsibilities. Further information is to be found here:

<https://cfl.mara.local/display/TEC/03-Change+Employee#tab-ENGLISH+VERSION>
<https://cfl.mara.local/display/TEC/Leaver+Process>

Objective A.6.6 Confidentiality or Non-Disclosure agreements

Requirements for confidentiality or non-disclosure agreements reflecting the organisation’s need to protect information shall be identified and regularly reviewed.

Panbet Curacao NV Information Security Policy

Objective A.6.7 Remote Working

Scope

This policy applies to all Members, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the Panbet Curacao NV network. This policy applies to implementations of VPN that are directed through an IPSec Concentrator.

Yubikey Policy

- Yubikeys are hardware security keys which must be used when accessing company's production environment and infrastructure servers with privileged rights.
- Yubikeys are received upon employment (with "New Starter" Jira task in SD project) or upon request from line manager (with task in SD project). For contractors, yubikeys are purchased by the contractor and are compensated in invoice, for other employees yubikeys are received from IT support directly or via mail.
- Instructions on setting up yubikey:
 - for ssh: <https://cfl.mara.local/display/MP/Yubikey+SSH#YubikeySSH-English+version>
 - for windows (AD): <https://cfl.mara.local/display/MP/Yubikey+AD#tab-English+version>

2FA miniOrange Policy

- miniOrange is identity and access management solution. It is used for two factor authentication when accessing corporate VPN network.
- *MiniOrange access is granted when a new employee has been given a new corporate laptop or BYOD policy has been signed.*
- *Further information can be found here:*

<https://cfl.mara.local/display/BRHR/Bring+Your+Own+Device+%28BYOD%29+Policy>
<https://cfl.mara.local/pages/viewpage.action?pageId=399725424>

VPN Policy

Approved Members and authorized third parties (contractors, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software and paying associated fees.).

Additionally:

1. It is the responsibility of Members with VPN privileges to ensure that unauthorized users are not allowed access to Panbet Curacao NV internal networks.
2. VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.

Panbet Curacao NV Information Security Policy

3. When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
4. Dual (split) tunnelling is NOT permitted; only one network connection is allowed for members of the IT Department.
5. VPN gateways will be set up and managed by the Panbet Curacao NV network administration groups.
6. All corporate devices connected to Panbet Curacao NV internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard. It is recommended that the connected computer runs the same antivirus software as the Panbet Curacao NV computers; this includes personal computers. Members' and agents' personal devices are monitored through SentinelOne agents, which trigger specific alerts and remove any threats automatically if unwanted software is installed.
7. VPN users will be automatically disconnected from Panbet Curacao NV network after 24 hours of inactivity. The user must then login again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
8. The VPN concentrator is limited to an absolute connection time of 24 hours.
9. For VPN access users of computers that are not PCNV-owned equipment must configure the equipment to comply with Bring Your Own Device policy. User must fill out the Bring Your Own Device file (BYOD file), which is located here: <https://cfl.mara.local/pages/viewpage.action?pageId=339252383#>. After filling out the file they need to create a task in ITSEC project (<https://jira.mara.local/projects/ITSEC/>) and attach the file to it. Upon receiving the file will be reviewed by IT Security department.
10. Only System Administrator/Network Manager/IT Department approved VPN clients may be used.

By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of Panbet Curacao NV network, and as such are subject to the same rules and regulations that apply to Panbet Curacao NV- owned equipment, i.e., their machines must be configured to comply with the company's Security Policies.

Panbet Curacao NV Information Security Policy

Objective A.6.8 Information Security Event Reporting

All Group employees are required to report all information security related events or any suspicions on information security related events to the IS department. Contact information is available in all mandatory trainings or in Confluence.

Standard – A.7 Physical Controls

Objective A.7.1 Physical Security Perimeters

Panbet Curacao NV have their relevant offices, all of them apply relevant physical security controls, where for Panbet Curacao NV the following apply and is not exhaustive.

- Unauthorised entry into buildings, rooms, or areas containing information assets is prohibited.
- The removal of assets without permission from the premises is unacceptable.
- The unauthorised utilisation of premises assets, such as computers and related devices, is not permitted.
- Unauthorised tampering with electronic communication equipment, such as telephones, faxes and computer terminals, is not allowed.

For more information, please contact your local premises manager or HR.

Objective A.7.2 Physical Entry

Panbet Curacao NV have their relevant offices, all of them apply relevant physical security controls. For more information, please contact your local premises manager or HR.

Objective A.7.3 Securing Offices, Rooms and Facilities

Panbet Curacao NV are processing high volumes of customer data. That is why Whiteroom policy have been developed. This is distinct area which is clearly sign-posted at every point of entry. Only specific employees have access, no digital devices are to be brought in, no files are to be carried out without written approval of a Head of Department. No photos or videos are to be taken within the Whiteroom premises.

<https://cfl.mara.local/display/ISHR/White+Room++Environment+Policy>

<https://cfl.mara.local/display/BRHR/White+Room++Environment+Policy>

Objective A.7.4 Physical Security Monitoring

The Company uses closed circuit television (CCTV) images to provide a safe and secure environment for employees and visitors to the Company's business premises and to protect the Company's property. A specific CCTV policy sets out the use and management of the CCTV equipment and images in compliance with the General Data Protection Regulation 2016/679 (EU), under the provisions of Article 89 of Organic Law 3/2018 of 5th December, article 20.3 of the Worker's Statute, the Data Protection Act 2018 and the Information Commissioner's Office CCTV Code of Practice.

<https://cfl.mara.local/display/ISHR/Video+Surveillance+Policy>

Panbet Curacao NV Information Security Policy

<https://cfl.mara.local/display/BRHR/CCTV+Policy>

Objective A.7.5 Protecting Against Physical and Environmental Threats

Panbet Curacao NV have their relevant offices, all of them apply relevant physical security controls. For more information, please contact your local premises manager or HR.

Objective A.7.6 Working In Secure Areas

As stated in A.7.3 Panbet Curacao NV have specific whiteroom policy. PCNV is committed to ensuring that all customer data is secure, in particular any data associated with customer financial information and payment cards.

<https://cfl.mara.local/display/ISHR/White+Room++Environment+Policy>

<https://cfl.mara.local/display/BRHR/White+Room++Environment+Policy>

Objective A.7.7 Clear Desk and Clear Screen

Equipment must be safeguarded appropriately – especially when left unattended. Users shall ensure that unattended equipment has appropriate protection. There is a unattended lock timeout which is set to 300s or 5 minutes. Any user security keys (smartcards/access cards/yubikeys) must be physically secured (i.e., locked in a desk drawer or filing cabinet, locked in an office, or taken away with them).

Objective A.7.8 Equipment Siting and Protection

Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access.

Server security

All internal servers deployed must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by the IT Department.

Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes a review and approval by the IT Department.

PCNV has developed a policy with regards to deploying new servers. It outlines what is to be done and the responsible personnel. The policy resides here:

<https://cfl.mara.local/pages/viewpage.action?pageId=18262673>

Objective A.7.9 Security of Assets Off-Premises

To protect information and equipment used outside of organisational premises, strict security measures are enforced. These include disabling insecure features (e.g.

Panbet Curacao NV Information Security Policy

WPS, remote web access), changing default passwords, applying regular updates, and securing Wi-Fi with strong encryption. Users must follow security policies such as locking devices when unattended, safeguarding access credentials, and ensuring confidential data is not exposed to unauthorised individuals in home or public environments. Further information can be found here:

<https://cfl.mara.local/display/SPHR/Portable+IT+Equipment+Policy>
<https://cfl.mara.local/pages/viewpage.action?pageId=165071991#>

Objective A.7.10 Storage Media

Removable data cannot be used during the software development/manufacturing process. In regards to the operation of software manufactured by Panbet Curacao NV, only taped libraries used can qualify as removable data. All these libraries are stored on a server hosted in certified datacentres (CLCs) thus datacentres procedures are applicable here. Cartridges are to be replaced by authorised personnel only and are to be stored in a secure safe at CLC before physical destruction takes place.

Disposed media is to be securely destroyed at CLC or an operational office depending on their location of use. All information of a confidential or sensitive nature must be securely destroyed when no longer required. The procedure for the destruction of confidential or sensitive records is as follows:

- Electronic files should be deleted in such a way that they cannot be retrieved by simply undoing the last action or restoring the item from the Recycle Bin.
- Destruction of backup copies should also be managed;
- Media and equipment should be physically destroyed prior to disposal;
- Paper should be mechanically shredded if the content is sensitive.

Changes of software version are to be controlled by a Panbet Curacao NV officer, with old versions to be stored at CLC and operational offices indefinitely. PCNV has developed a specific policy with regards to Media Disposal.

Objective A.7.12 Cabling Security

The data centres utilise multiple network switches. Access restrictions are enforced on network ports that are publicly accessible. Personnel with access to the premises are assigned different levels of physical and designated access based on their roles. Additionally, CCTV cameras are strategically positioned at key locations to ensure comprehensive coverage of the perimeter.

Objective A.7.14 Secure Disposal or Re-Use of Equipment

All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal. The data residing on the devices is to be categorized – Low/Moderate/High. Depending on its categorization a number of actions are to be taken. A TEC Jira task is to be created as well. Further information can be found here:

Panbet Curacao NV Information Security Policy

<https://cfl.mara.local/pages/viewpage.action?pagelId=152450037>

<https://cfl.mara.local/display/ITSEC/Media+Sanitization>

Standard – A.8 Technological Controls

Objective A.8.1 User Endpoint Devices

Panbet Curacao NV has developed a policy with regards to Mobile Computing.

Special security issues that relate to mobile devices include the following:

- a) Any malware (viruses, worms, Trojans) that infect the device can bypass the companies' security and spread rapidly to other devices once connected back to the network;
- b) If data stored on a mobile device is not backed up by the user it could be completely lost if the device is stolen or fails;
- c) Any sensitive data stored on a mobile device would be compromised should it be stolen or lost.

The following security controls, when available, must be activated on all devices to help protect against theft of sensitive information contained on the device:

- a) Where sensitive information is held on laptops or mobile storage devices, data encryption must be applied to that information or to the entire device.
- b) All mobile devices must have a password protected keyboard/screen lock that is automatically activated by a period of inactivity. The inactivity time interval should be no more than 10 minutes.
- c) When Members are not at their desk for an extended period of time the device must be physically secured (i.e., locked in a desk drawer or filing cabinet, locked in an office, or taken away with them).
- d) When travelling, the following is recommended practice where possible;
 - Keep devices in own possession at all times.
 - Do not put devices in checked baggage and be aware of the possibility of theft when going through security checkpoints at airports.
- e) When using a laptop, do not process personal or sensitive data in public places e.g. on public transport.
- f) Passwords for access to systems should never be stored on mobile devices where they may be stolen or permit unauthorized access to information assets.
- g) If mobile device, or sensitive information, is stolen or lost, loss has to be reported, as quickly as possible, to IT administrator or CTO.

Panbet Curacao NV Information Security Policy

1. Device security:

Corporate teams:

Prioritize the use of company-provided equipment, configured with appropriate security policies.

Keep operating systems and applications up to date with the latest security patches.

Deploy up-to-date antivirus and anti-malware software.

Encrypt hard drives to protect information in the event of loss or theft of the device.

Personal devices (BYOD):

Establish clear policies on the use of personal devices for work.

Require the installation of security software and the configuration of strong passwords.

Implement mobile device management (MDM) solutions to control and protect corporate data.

What is more a specific procedure for device security settings have been developed. It defines what is to be done for Windows, macOS, Linux, Android and iOS devices.

The procedure resides here:

<https://cfl.mara.local/pages/viewpage.action?pageId=339252383>

2. Network security:

Secure connections:

Require the use of secure Wi-Fi networks and avoid unprotected public networks.

Implement the use of virtual private networks (VPNs) to encrypt the connection and protect data transmission.

Firewall:

Enable and properly configure the firewall on devices.

Deploy hardware firewalls on the home network if possible.

3. Authentication and access:

Strong passwords:

Require the use of complex and unique passwords for all accounts.

Implement multi-factor authentication (MFA) whenever possible.

Access Control:

Limit access to information and systems to authorized users only.

Implement the principle of least privilege, granting only the necessary permissions for each task.

4. Data protection:

Panbet Curacao NV Information Security Policy

Device Encryption

- All endpoints that store or process personal data must use full disk encryption (e.g., BitLocker, FileVault, or native Android/iOS encryption).
- External drives or USB devices must be encrypted or authorized by the IT Security Department.

Strong Authentication and Session Control

- Login with unique and strong credentials is required.
- Multi-factor authentication (MFA) is mandatory for all devices accessing corporate resources.
- Automatic session lock must be configured after a maximum of 5 minutes of inactivity.

Centralized Management and Configuration

- All devices must be managed through a Mobile Device Management (MDM) or Enterprise Mobility Management (EMM) solution.
- Centralized enforcement of security policies, encryption, antivirus, installation restrictions, and remote wipe capabilities.

Antivirus and Antimalware Protection

- Mandatory installation of up-to-date antimalware solutions.
- Centralized monitoring and alert management by the Security Team.

Updates and Patching

- Automatic and enforced updates of operating systems and critical software.
- Centralized control to verify the security patch status of all endpoints.

Application Control

- Only applications approved by the organization (whitelisted) may be installed.
- Applications must be obtained solely from official or internal repositories.

Activity Logging and Monitoring

- Local and centralized logging of access, errors, critical events, and connections to internal resources.
- Monitoring to detect anomalous activity or signs of unauthorized access.

External Devices and Removable Media Restrictions

- Control and restriction of the use of USB devices or other external storage media.

Panbet Curacao NV Information Security Policy

- Mandatory encryption of any medium used to transfer personal data.

Separation of Personal and Work Environments (on BYOD devices)

- Logical separation using secure containers for corporate data and applications.
- Ability to selectively wipe corporate data without affecting the user's personal data.

Incident Response and Remote Wipe

- Capability for remote data wiping in case of loss, theft, or security incident.
- Automated procedures for isolating compromised devices.

Device Risk Assessment

- Risk classification for each type of endpoint and implementation of proportional controls based on the nature of data and functions processed.
- Periodic review of compliance with technical measures through audits.

5. Awareness and training:

Safety Training:

Provide regular training to employees on security best practices in remote work. Raise awareness of the risks of phishing, malware, and other cyber threats.

Clear policies:

Establish clear policies on the use of computer and mobile equipment in teleworking. Communicate policies clearly and concisely to all employees.

6. Mobile Device Security:

Screen lock:

Turn on automatic screen lock with password or biometrics.

Updates:

Keep the operating system and applications up to date.

Secure Applications:

Download apps only from official sources.

Remote Erase:

Set up the remote wipe feature in case your device is lost or stolen.

[Mobile computing and communications](#)

[Issuing Policy](#)

Company Communication Devices (“**CCDs**”) shall be issued exclusively to personnel whose job responsibilities necessitate immediate and frequent communication while

Panbet Curacao NV Information Security Policy

away from their primary work locations. For the purposes of this policy, CCDs are defined to include handheld wireless devices, cellular phones laptops and any other mobile devices used to connect to Panbet Curacao NV's internal networks. The distribution of such devices must be carefully controlled to ensure that the productivity benefits justify the associated costs.

Handheld wireless devices may be issued to personnel whose roles require immediate and critical communication to support PCNV business operations. Typically, these individuals hold executive or management-level positions and remote workers. In addition to facilitating verbal communication, these devices must enable users to review critical information and provide documented responses to urgent issues.

Bluetooth

Hands-free communication devices, including Bluetooth-enabled accessories, may be issued to personnel upon approval by the appropriate management authority. When utilizing Bluetooth devices, especially during pairing processes, users must exercise caution to prevent unauthorized access or interception of communications.

Employees must avoid pairing Bluetooth devices in areas where sensitive conversations could be recorded or intercepted. Users should also be aware that certain Bluetooth devices can operate over extended distances—up to approximately 800 feet (240 meters)—depending on the class and environmental conditions.

All Bluetooth usage must comply with PCNV's security standards to protect company information and communications.

Modern Bluetooth standards (e.g., Bluetooth 5.0 and above) offer enhanced security; however, users must remain vigilant, particularly in public or unsecured environments. Although modern standards provide improved security, vulnerabilities still exist. Employees must be aware of potential threats, including:

- Bluesnarfing: Unauthorized access to a device via Bluetooth to steal information such as contacts, messages, emails, or files.
- Bluebugging: Attackers take control of a Bluetooth-enabled device to eavesdrop on conversations, send messages, or make unauthorized calls.
- Bluejacking: Sending unsolicited messages to nearby Bluetooth devices, potentially used for phishing or harassment.

Security Precautions:

- k) Keep Bluetooth turned off when not actively in use.
- l) Always pair devices in secure, private environments.
- m) Use strong authentication and avoid using default or easily guessable PINs.
- n) Disable Bluetooth discoverability except when actively pairing a device.
- o) Regularly update device firmware to patch known Bluetooth vulnerabilities.
- p) Unpair and remove any unknown or untrusted devices immediately.

Panbet Curacao NV Information Security Policy

Failure to apply these precautions could expose PCNV to significant information security risks.

Personal Use

CCDs and associated services, including voicemail, are provided primarily for the purpose of conducting official company business. Personal use of these devices is permitted only on a minimal and incidental basis, provided that such use:

- Does not interfere with business operations or employee productivity;
- Does not result in significant additional costs to the company;
- Does not involve activities that violate company policies, applicable laws, or ethical standards; and
- Does not compromise the confidentiality, integrity, or availability of company information.

Employees must understand that all communications and data transmitted, received, or stored using CCDs and voicemail systems remain the property of PCNV and may be subject to monitoring and review in accordance with applicable laws and internal policies. Users should have no expectation of personal privacy when utilizing company-issued devices. Misuse or excessive personal use may result in disciplinary action, up to and including termination of employment.

PCD Safety

Conducting telephone calls or utilizing PCDs while driving can be a safety hazard. Drivers should use PCDs while parked or out of the vehicle. If Members must use a PCD while driving, the company requires the use of hands-free enabling devices. PCDs should not be connected to the company's network. In the event PCD connection to the network is required, written approval must be obtained by the CEO or CTO. PCDs must be made available for inspection and remote wiping if requested to do so. The PCD must also be password protected.

Objective A.8.2 Privileged Access Rights

The allocation and use of privileges shall be restricted and controlled and have to be based on roles. Changes in privileges are normally made based on business process changes and introductions of new roles..

1. Principle of least privilege:

This is the main foundation of privilege management. It states that each user or entity should be granted only the permissions necessary to perform their specific tasks, avoiding unnecessary access.

2. Role-based access control:

Panbet Curacao NV Information Security Policy

Users are assigned roles based on their responsibilities and roles within the organization.

Each role has a set of permissions and access rights associated with it.

This simplifies privilege management and ensures that users have access to only what they need.

3. Privileged Account Management:

Accounts with elevated privileges, such as administrator accounts, require special attention.

Additional security measures are implemented to protect these accounts, such as multi-factor authentication and activity monitoring.

4. Audit and registration:

Detailed records are maintained of all activities related to privilege management.

This allows for regular audits to detect potential irregularities or security breaches.

5. Regular review and updating:

Access privileges should be reviewed and updated regularly to accommodate changes in user roles and organizational infrastructure.

This ensures that the privileges granted remain appropriate.

Objective A.8.3 Information Access Restriction

Employee User Inactivity Timeout

The system implements a user inactivity timeout system. The VPN concentrator is limited to an absolute connection time of 24 hours. Access to information and application system functions by support personnel shall be restricted in accordance with the defined access control policy.

Access to information and application system functions by users and support personnel shall be restricted in accordance with the defined access control policy.

Customer User Inactivity Timeout

The system implements a user inactivity timeout system. When in the preferences window after registration, the customer is able to specify the session inactivity timeout. The inactivity timeout counter will be implemented from the client's browser.

Should connection with the server be lost for any reason, the user will be informed of the loss of connection should they subsequently perform an action which requires connection to the server. In the event of this happening the user will be required to login again before they are able to place further bets.

Objective A.8.4 Access to Source Code

Access to Source Code in Panbet Curacao NV is governed by the Head of Development department, subject of review and approval by Technical Compliance and ITSEC departments.

Objective A.8.5 Secure Authentication

Access to operating systems shall be controlled by a secure log-on procedure.

Panbet Curacao NV Information Security Policy

Logon to operating systems are allowed only via centralized authentication mechanisms (Active Directory for Windows workstations and servers, LDAP for Linux stations and network equipment). User sessions are automatically logged off after a period of inactivity equal or less than 10 minutes depending on the employee's role. Access to specific objects is granted based on group membership, therefore it is always possible to know what objects the user can access.

Last user name shall not be stored in log-on window. Secure log-on pop-up message of the following content to be displayed: This computer system is the property of (company name). It is for authorized use only. By using this system, all users acknowledge notice of, and agree to comply with, the IT Security Policy. Unauthorized or improper use of this system may result in administrative disciplinary action, civil charges/criminal penalties, and/or other sanctions. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this warning.

Each user is assigned a unique identifier (username) and a password. Complexity requirements for the password are implemented in the centralized password management system (AD and LDAP).

Objective A.8.7 Protection Against Malware

Malicious codes can be programs such as viruses, worms, Trojan applications, and scripts used by intruders to gain privileged access, capture passwords or other confidential information e.g. user account information. Malicious code attacks are usually difficult to detect as certain viruses can be designed to modify their own signatures after infecting a system and before spreading to another. Some can also modify audit logs in order to hide unauthorised activities.

The following are some examples of malicious code attacks:

1. Worms or viruses rapidly spreading through emails (e.g. I Love You, Melissa Virus);
2. Spying codes (e.g. Caligula Virus, Marker Virus, Groov Virus);
3. Remotely controlled codes (e.g. Back Orifice, NetBus); and
4. Coordinated attack codes (e.g. Trinoo, Tribe Flood Network (TFN)).

Panbet Curacao NV ("PCNV") and its Members which include directors and board members of Panbet Curacao NV, employees of Panbet Curacao NV through the use of recognised industry best practice and through education, seeks to minimise the risks from Malicious codes. Furthermore, seeks to minimise the risks of computer viruses through education and good practice/procedures.

PCNV has implemented SentinelOne and Kaspersky Enterprise Security agents within our environments. SentinelOne MDR (Managed Detection and Response) and

Panbet Curacao NV Information Security Policy

XDR (Extended Detection and Response) are security solutions designed to protect endpoints, networks, and cloud environments from advanced threats. In essence, SentinelOne MDR offers expert-managed services for monitoring and responding to threats, while SentinelOne XDR expands detection and response capabilities across a broader range of data sources and security layers, using automation and advanced analytics to identify and mitigate threats more effectively. On the other hand, Kaspersky Enterprise Security is a comprehensive suite of cybersecurity solutions designed for businesses to protect their IT infrastructure from a wide range of threats. What is more we have email protection supplied by Kaspersky Mailgate.

Mobile codes are a deliberate attempt to destroy or damage data on a computer system. They are transmitted in software, which is innocently loaded onto a computer and can lead to complete loss of data on that system.

Objective A.8.8 Management of Technical Vulnerabilities

Panbet Curacao NV has developed a policy with regards to Management of Technical Vulnerabilities. Technical vulnerabilities are proactively managed through regular scanning, asset inventory maintenance, and timely patching. Identified risks are evaluated and remediated based on severity and business impact, following defined change management procedures. The organisation also conducts penetration testing and collaborates with vendors and third parties to stay informed about emerging threats.

In addition, in alignment with GDPR obligations, any technical vulnerability that results in a personal data breach is subject to the organisation's Data Breach Notification Procedure. This ensures that, where applicable, the Spanish Data Protection Authority (AEPD) and affected data subjects are notified within the required timeframes. The procedure defines clear responsibilities, timelines, and documentation requirements to ensure regulatory compliance and mitigate potential impacts on individuals.

Objective A.8.9 Configuration Management

System Administrators

Sysadmins are primarily responsible for configuration management. This is achieved using tools such as Rudder, which provides centralised configuration enforcement, and Ansible, which is used for automating provisioning and repetitive tasks across systems.

Duty Administrators

Dutyadmins handle deployment activities and operational checks. They use cURL to fetch deployment artifacts from storage and rely on common administrative tools (e.g., Tomcat scripts) for managing application lifecycles, such as starting and stop-

Panbet Curacao NV Information Security Policy

ping services. Following a restart, Dutyadmins perform health checks by reviewing status pages and inspecting application logs to ensure successful deployment and system stability.

DevOps Engineers

DevOps teams manage and maintain the CI/CD pipelines that facilitate continuous integration and delivery. The pipeline typically follows this flow:

GitLab (pipeline trigger) → Git commit to Helm chart repository → ArgoCD → Kubernetes (K8s) deployment

This streamlined process allows code changes to be automatically packaged, promoted, and deployed to Kubernetes clusters, ensuring faster delivery cycles and improved consistency across environments. Once the legal storage periods have expired, the information will be deleted.

Objective A.8.10 Information Deletion

Data deletion is performed using a secure three-pass method: two passes with zeros and one with pseudo-random data. For local disks, tools like `/dev/zero`, `sg_sanitize` (for SAS/SSD), and `hdparm` (for SATA SSDs) are used. Drives must be removed from RAID arrays and visible as standalone devices. BLOCK ERASE is preferred for SSDs for faster, hardware-level deletion. Once the legal storage periods have expired, the information will be deleted.

Objective A.8.11 Data Masking

All Panbet Curacao NV are utilizing their relevant Data Masking processes for sensitive information like Bank Card numbers, Personal Information and etc.

Objective A.8.12 Data Leakage Prevention

To prevent unauthorized disclosure of sensitive information, Data Leakage Prevention (DLP) features built into the Microsoft 365 suite are actively used to monitor and control data sharing across email, cloud storage, and collaboration platforms. In addition, the use of USB mass storage devices has been restricted across the organization to reduce the risk of data exfiltration via removable media.

Objective A.8.13 Information Backup

All Panbet Curacao NV have main Oracle Databases that store all critical information, including personal data. To ensure the backing up of the databases, Oracle Data Guard service is deployed (described below). This service ensures that all Oracle Databases are backed up in real-time/almost real-time way to secondary cluster nodes that are readily available in case that the primary nodes failed. The process is part of the High Availability of the Data Base services as well as the data itself and is implemented in resilient way with minimal Data Base service disruptions in case of issues. The restoration process is being tested and performed in full on a weekly or bi-weekly

Panbet Curacao NV Information Security Policy

process and is governed by the “Deploy” process and includes switching the primary Database cluster Node to the secondary Database cluster Node, performed testing by various departments and work in production for the time being of the “Deploy” process. When this process is completed and after no issues are identified, the secondary cluster node (now primary) is being returned to primary and only then the “Deploy” process is considered as completed. In case of issues are identified, the Deploy is rolled back and a PIR (Problem Investigation Report) Jira task is created where a root cause analysis is performed, corrective actions are performed, and preventive actions are suggested to the relevant Head of Department or Team Lead to be applied if approved.

Objective A.8.14 Redundancy of Information Processing Facilities

All Panbet Curacao NV are using multiple Data Centers to provide redundancy of the processing facilities where all are located in different Geographical locations. The office locations are covered by the ability to work remotely in case of emergencies and relevant Policies and Procedures apply based on the relevant location. Those are managed and distributed by HR.

Objective A.8.15 Logging

Audit logs recording user activities, exceptions and information security events shall be produced and kept for an agreed period with Compliance department to assist in future investigations and access control monitoring. The period to retain logs is 6 years.

A multi-level audit with a minimum of the following measures is to be implemented (with a reference to system time):

- Recording (in chronological order) all user actions;
- Results of all operations executed on the system;
- System events and errors;
- Logs of interaction with external services.

In order to facilitate audit logs recording user activities, system security events and general audibility, a Wazuh SIEM system has been employed. It retains security logs for 12 months. Further information can be found here:

<https://cfl.mara.local/display/PIR/Wazuh>

Logging facilities and log information shall be protected against tampering and unauthorised access. A minimum of the following measures are to be implemented:

- System logs to be stored on a separate partition of the disk system at data-centre;
- Access restricted to authorised personnel of IT department;
- System interaction logs, including users actions logs, to be stored in the central database;

Panbet Curacao NV Information Security Policy

- Access rights to the system interaction logs to be determined by database administrators and user rights.

System administrator and system operator activities shall be logged. To implement the following definitions:

- Administrator's logs are part of the system logs;
- Operator's logs are user actions logs (described above in 10.10.3).

Faults shall be logged and analysed and appropriate action will be taken with regard to the software manufacturing process taking into consideration the following rule:

- Separate, debug and production logging to be applied to all programming components during development process.

In relation to the manufactured software (production/operations) the following has to be applied:

- Fault Reporting /Problem Reporting and Management Procedures;
- Any apparent problems with the software operation to be picked up by the Customer Service Centre staff (through software usage) of Panbet Curacao NV;
- These problems to be escalated the IT department;
- System administrators also to be able to detect problems through system monitoring, and try to resolve the problem accordingly;
- All problems to be recorded in a bug tracker, along with information on the software version, problem escalation and resolution issues;
- This log to be managed by the IT Department and should contain both problems caught by the system operators and maintenance teams.

Objective A.8.16 Monitoring Activities

Systems monitoring will be performed using a number of tools. These will monitor connectivity, database, security and other issues. Monitoring, and where applicable, problem resolution, will be performed from the Panbet Curacao NV.

The IT Department will deal with any problems caused by system malfunctions of non-gaming equipment. There will be a readily available list of contact telephone numbers for all companies and their helplines for each piece of equipment which is integral to the operation of both Panbet Curacao NV's gaming system and Customer Service Centre operations.

Access to all aspects of the gaming system including the IDS is managed remotely. Connections to the IDS are filtered by IP address on the firewall. Access to any of the gaming system elements are granted to members of the system administration department.

To ensure data integrity, availability, resiliency and maintainability the IBM DS 3524 Disk Array is used. It provides redundant components (disks, controllers, power supplies, fans etc.) thus eliminating single points of failure from the system architecture.

Panbet Curacao NV Information Security Policy

Disk array monitoring is performed through the use of in-built SNMP procedures.

System monitoring is performed with Zabbix monitoring tool through the use of zabbix-server, zabbix-proxy, Postgresql, logstash, custom plugins for zabbix.

Hardware Monitoring is performed with the help of Dell Remote Access Controller (DRAC). DRAC is a specialized monitoring and support system specifically designed to work with DELL equipment, independent of the underlying operating system. Equipment monitoring can also be performed automatically through Zabbix.

Advanced Intrusion Detection Environment (AIDE) will be used to detect and mitigate intrusions into the system. A database is created after the software is run for the first time, which thereafter checks the integrity of protected files. This ensures that after database initiation and other additional checks (performed by the system administrators), are made against the controlled sums of protected files and in the case of any changes being detected the information is saved in a log and sent off in an email to the system administrator. Control over the system configuration files located in the /etc directory are protected with the help of AIDE.

The Intrusion Detection checksum and any subsequent checks are logged to the syslog server, access to which permitted only for the system administration group via SSH. Open access across the network will be forbidden.

Further information with regards to the Monitoring technologies employed is to be found here:

<https://cfl.mara.local/pages/viewpage.action?pageId=7733290>

Objective A.8.17 Clock Synchronization

Each server has to synchronise clock using ntp protocol with *.pool.ntp.org.

Datacentre: all servers and network equipment have to synchronise using this methodology.

Office environment: Active Directory servers and network equipment are synchronised with *.pool.ntp.org; workstations are synchronised with Active Directory servers and network equipment

Objective A.8.18 Use of Privileged Utility Programs

Most computer installations have one or more system utility programs that might be capable of overriding system and application controls. Use of these system utility programs must be restricted and tightly controlled. The following controls should be considered:

- use of authentication procedures for system utilities;
- segregation of system utilities from applications software;

Panbet Curacao NV Information Security Policy

- limitation of the use of system utilities to the minimum practical number of trusted authorized users;
- authorization for ad hoc use of systems utilities;
- limitation of the availability of system utilities, e.g. for the duration of an authorized change;
- logging of all use of system utilities;
- defining and documenting of authorization levels for system utilities, and
- removal of all unnecessary software based utilities and system software.

Objective A.8.19 Installation of Software on Operational Systems

All Panbet Curacao NV software is to be installed only by authorized IT Support personnel.

Objective A.8.20 Networks Security

Control and management of the equipment is performed by a limited number of staff with the necessary qualification and security permission. Remote access is controlled via SSH keys, AD certificates, user name and password driven system, with access to the equipment granted to authorized networks.

Physical access to the equipment is restricted to members of the system administration and IT departments. All non-used ports are shut down

The production system hardware that has Panbet Curacao NV manufactured software installed is located in the data centre, thus all physical hardware management will be performed from there.

Remote Management of production servers will be performed by the appropriate internal IT department. Remote management is performed with the help of the SSH protocol. Access to the system is only granted to the members of the system administration and maintenance departments. To prevent unsanctioned access to the system, connections are secured using VPN IPSec. Each system administrator has a unique user name and password.

PCNV has employed technologies like YubiKey and miniOrange.

A firewall is in place for all incoming and outgoing connections. Only required ports are open. Violations are logged using a syslog server. Network packet capture is performed to a rotated log for audit purposes.

Network equipment is physically accessible only by authorized personnel. In addition to that, authentication is enforced on management ports of the equipment to prevent unauthorized access.

Equipment in the network is identified by its address. A number of L2 security mechanisms (DHCP snooping and MAC security) are in place to prevent unauthorized address assignment to workstations and other equipment.

Panbet Curacao NV Information Security Policy

Only authorized users are allowed to access network resources. This is enforced by active network equipment, such as firewalls (for layer 3 and above) and switches (for layer 2).

Objective A.8.21 Security of Network Services

General guidance

Security features, service levels and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in -house or outsourced.

Details

System administration and maintenance requires varying levels of access and permissions. To ensure auditability during system use, all user operations are logged on the following tasks and levels:

- Authentication, authorization and access to the firewall;
- Authentication and authorization in the operating system;
- Application Servers;
- Web Servers;
- Database Servers;
- FTP Server;
- Mail Transfer Agent;
- Network Management Services;
- Monitoring of unauthorized connections to the network is performed using standard means provided by the operating system and VPN;
- Connection monitoring from unauthorized hardware is managed by the system administrators with the aid of the arpswatch utility, which is an open source program and performs monitoring Address Resolution Protocol (ARP). The main job of this utility is to control ARP activity for any ARP spoofing;
- Connection to the system is only possible after the user has been authorized. Connection to the system with the use of a USB device is not possible as USB ports are disabled.

The following system components are set in read only mode:

- Firewall;
- Network Adapter Modules;
- Switches.

The following system components are set in read/write mode:

- Application server with its Ethernet interfaces;
- Database server with its Ethernet interfaces.

Management and auditability of access and modifications to network machines are performed by the following tools:

Panbet Curacao NV Information Security Policy

- VPN – for limiting access from external networks;
- IPSec – for network traffic encryption;
- Cisco Adaptive Security Appliance Software Version 8.2(3)– for management and auditability of network access;
- Firewall event logging subsystem;
- Operating system, application server and database server event logging subsystems.

External access to the network is only allowed via VPN. VPN policy enforces user authentication via common authentication mechanisms (AD/LDAP). Two-factor authentication must be used.

Objective A.8.22 Segregation of Networks

Sensitive systems shall have a dedicated (isolated) computing environment.

The network is divided into production, development and management parts. The segregation is done via VLAN and routing/firewalling between logical segments.

Dynamic routing disables the network interfaces where no dynamic routing is expected. Routing filters are applied on external interfaces to prevent address spoofing.

Objective A.8.23 Web filtering

Web filtering is applied based on job roles assigned to relevant Active Directory group memberships. The process is governed by IS, TC and IT departments.

Objective A.8.24 Use of Cryptography

Requirements for ensuring authenticity and protecting message integrity in applications shall be identified and appropriate controls (like TLS encryption or an equivalent) shall be implemented.

We are using SecureDoc disk encryption for developers -

<https://winmagic.com/en/home/> Furthermore, cryptography is used for storage of passwords hashes, when sending requests to external processing systems and while creating VPN tunnels. There are different specific requirements depending on the payments systems in accordance with their specific protocols. Algorithms described below are used here for code creating.

Cryptographic controls are described in the Panbet Curacao NV Cryptographic Policy.

Objective A.8.25 Secure Development Life Cycle

PCNV has developed a policy which resides here:

<https://cfl.mara.local/display/GPP/Panbet+Curacao+NV> and implemented SDLC processes employing industry-accepted standards. The list of industry-leading security

Panbet Curacao NV Information Security Policy

standards, benchmarks and frameworks to use includes but is not limited to the following:

- The United States Department of Justice Systems Development Life Cycle <http://www.usdoj.gov/jmd/irm/lifecycle/table.htm>
- The Open Web Application Security Project (OWASP) <http://www.owasp.org>
- National Institute of Standards Technology (NIST) <http://www.nist.gov>

PCNV employs a number of structured software development processes and phases, which include properly authorizing, testing, approving, implementing, documenting and maintaining the specified system/application. All SDLC activities, ranging from the initial requirements stage to the routine maintenance of a system/application, are administered by Panbet Curacao NV employees, located at their respective offices.

The SDLC methodology encompasses a number of phases, each concluding with a major milestone. Assessments are conducted after each phase to determine if objectives have been satisfied. Panbet Curacao NV utilizes skilled software engineers throughout all phases, which results in a thorough and uninterrupted process from beginning to end.

Objective A.8.26 Application Security Requirements

Information involved in all types of online transactions—including the transmission of personal data—shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, disclosure, duplication, or replay. Security requirements for such transactions should be integrated throughout the Software Development Lifecycle (SDLC), including DevSecOps practices, starting from the requirements phase through to design, development, testing, deployment, and maintenance. This includes applying principles such as Security by Design and Security by Default, and incorporating secure development practices such as code reviews and automated security testing (e.g., SAST, DAST, IAST). All relevant stakeholders—including development, security, quality assurance, and business teams—should collaboratively define and regularly update security requirements in line with legal, regulatory, and technical changes. These requirements must be thoroughly documented, with clear traceability to implementation and validation evidence such as test results and approvals. Compliance testing must confirm correct implementation of controls prior to production deployment and after significant changes. Furthermore, ongoing risk assessments and vulnerability management should be conducted to evaluate potential threats and their impact on defined security requirements.

Transaction Security Policy

The withdrawal of funds from a customer's account to an external source such as a card can only be performed to the bank card payment method which was used to initially deposit funds into the system. It is only possible to change a card payment method registered to a particular account (except if the only change is to the expiry

Panbet Curacao NV Information Security Policy

date and/or issue number for credit/debit cards) when the account balance is equal to zero and the customer has no outstanding bets in the system.

All withdrawals from customer accounts to registered bank cards are performed through the payment system. When a customer requests a withdrawal from the site, their withdrawal is placed in a queue, which is then checked by the Payments department. The transaction is then sent to the customer's registered payment method. All communication with the payment systems are performed over the secure HTTPS protocol. Additional security measures are taken such as timeouts and request source IP checking on behalf of the payment gateways. When transferring funds to a customer's account, the customer is required to re-enter their password and CVN number.

Other fund transfer methods such as bank transfers etc. are performed by the customer support centre operators upon request by the customer (subject to authorization). All changes to a customer's balance and external payment sources are recorded within the system and can be viewed in the transaction history both from the web and desktop clients.

Data input to applications shall be validated to ensure that this data is correct and appropriate.

Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate in the circumstances

Information involved in electronic commerce passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorised disclosure and modification.

1. Authentication and authorization:

- Implementation of robust authentication systems, such as two-factor authentication (2FA), to verify the identity of users.
- Role-based access control to limit access to sensitive information to authorized personnel only.

2. Fraud prevention:

- Fraud detection:
 - Use of fraud detection tools to identify suspicious patterns in transactions.
 - Implementation of address verification systems and CVV codes to validate the authenticity of credit cards.
- Risk Management:
 - Conducting regular risk assessments to identify and mitigate potential vulnerabilities.
 - Implementing risk management policies to effectively respond to security incidents.

3. Infrastructure security:

- Network Security:

Panbet Curacao NV Information Security Policy

- Implementation of firewalls and intrusion detection systems to protect the network against external attacks.
 - Conducting regular penetration tests to identify and fix vulnerabilities.
- Application Security:
 - Development of secure web applications following security best practices.
 - Performing application security testing to identify and fix vulnerabilities.
- Server security:
 - Up-to-date maintenance of servers with the latest security patches.
 - Implementation of backup systems to ensure data recovery in the event of incidents.

Objective A.8.28 Secure Coding

PCNV has an official Secure Coding Policy which resides here:

<https://cfl.mara.local/display/GPP/Panbet+Curacao+NV> in order to ensure that the software development and secure coding policy and procedures adhere to the following conditions for purposes of complying with the regulatory requirements:

- Software developers involved in the System software development process will adhere to professional guidelines, such as the Open Web Application Security Project (OWASP) Code of Ethics and CWE/SANS.
- Panbet Curacao NV's software development lifecycle includes policies, processes and procedures to ensure that internally-developed System applications are not vulnerable to the following threats:
 - Injection Flaws (SQL, OS and LDAP Injection)
 - Buffer Overflows
 - Insecure Cryptographic Storage
 - Insecure Communications
 - Improper Error Handling
 - All high risk vulnerabilities identified in the vulnerability identification process as found in the Risk Ranking Table within the Security Patch Management Installation Policy and Procedures document.
 - Cross-Site Scripting
 - Improper Access Control
 - Cross Site Request Forgery
 - Broken Authentication and Session Management
 - All "High" vulnerabilities and threats as identified in the Risk Ranking Table found in the Security Patch Management Installation Policy and Procedures.

Objective A.8.31 Separation of Development, Test and Production Environments

Development test and operational environments shall be separated to reduce the risks of unauthorised access or changes to the operational system.

Panbet Curacao NV Information Security Policy

The following controls should be considered as a minimum:

- Development and operational software should run on a different computer processor, or in different domains or directories.
- Development and testing activities should be separated in the best and most appropriate way possible.
- Compilers, editors and other system utilities should not be accessible from operational systems.
- Different log-on procedures should be used for operational and test systems to reduce the risk of error. Users should be encouraged to use different passwords for these systems and menus should display appropriate identification messages.
- Development staff should only have access to operational passwords where controls are in place for issuing passwords for the support of operational systems. Controls should ensure that such passwords are changed.
- New features (source codes) are developed in a secure offline local environment and are continuously integrated into an offline source controlled environment change-managed by the development team. Only those developers who require access to these source codes are permitted access. When a feature is ready, it is promoted to a development environment which serves to provide the most up-to-date version of the feature to those who are not involved in its development but require access. An audit log of all accesses to source codes is maintained. This source controlled environment means that old versions of source code and the dates they were retired are retained.
- After feature completion, the development environment is promoted to a logically separate staging environment which mirrors the exact same environment as that of the live website. Performance within the staging environment is crucial because it reflects performance in the live environment more faithfully than the development environment.
- The final stage of development includes promotion to the live environment following a strictly controlled Change Management process.
- Access to production environment and databases is based on user roles definition and users access rights. Definition of segregation of duties is applicable to all Members, including IT support group. This Policy explicitly states that irrespective of all other arrangements and irrespective of the fact that all sensitive data in the databases is encrypted members of IT support group can have view only customers (punters data) database access rights.

Panbet Curacao NV Information Security Policy

- Copies of the source code, or of binaries or other formats that allow subsequent deployment and auditing, of the software elements of all software versions that have been used in the technical system actually used in the last four years shall be kept. The Directorate-General for the Regulation of Gambling may establish the obligation that the procedure for storing copies of the software elements includes a fingerprint of the same.

PCNV has developed policies with regards to Test and Development environments and their deployment and maintenance. Further information can be found here:

<https://cfl.mara.local/display/COEQA/Test+Environments>

<https://cfl.mara.local/pages/viewpage.action?pageId=311051616>

<https://cfl.mara.local/display/COEQA/Dev+Tests>

Objective A.8.32 Change Management

Panbet Curacao NV has a specific Change Management procedure. It is to control major and fundamental changes to the IT infrastructure and services; ensuring standardised methods and procedures are used for handling of changes within the organisation. The policy outlines how a Change Request is to be done, the roles of the people responsible for its management and the relevant authorities. The policy resides here:

<https://cfl.mara.local/display/GPP/Panbet+Curacao+NV>