Information Security Policy

Version 13.5

IT Security

Document attributes

Document Type:	*Política multi área*
File Name:	*Information Security Policy*
Document Code:	*POL-MUL_01*
Version:	*13.5*
Date:	*09/09/2020*
Author:	*IT Security*

Review, approval

Reviewed by:	*Javier Torres Alonso*	**Date:**	*11/10/2020*
Reviewed by:	*Mariano Blanchard*	**Date:**	*21/12/2021*
Approved by:	*EXCO*	***Date:***	*17/02/2022*

Change history

Version	Date	Description
12	04/19/2019	Update and changes
13	09/09/2020	Corrections
13.1	09/18/2020	Changes
13.2	12/10/2020	Final version
13.3	25/05/2021	Key Revocation and Wi-Fi Protocols update
13.4	*17/02/2022*	EXCO approval
13.5	*25/05/2022*	Backup Policy

- INDEX-

1 INTRODUCTION

Information Security is a business risk management challenge. Failure to protect **AFB** information could result in financial loss and have a negative impact on **AFB**'s brand.

The information, IT systems and network which support it are important assets for the business. Its availability, integrity, and confidentiality are essential for maintaining a competitive advantage, securing profitability, ensuring compliance with legal norms, and for the Group's own image. We are faced with risks from different sources. Our systems can be targeted by different threats, such as IT fraud, industrial espionage, sabotage, vandalism and natural phenomena, as well as technical issues such as system viruses or hackers.

All these threats are continuously expanding. This, added to the progressive sophistication of IT systems and business dependence, exposes **AFB** systems to increasing risks, which, if not managed correctly, can increase our vulnerability and subsequently affect our assets.

1.1 Objectives

The **AFB** Information Security Policy and Standards establish clear and concise security baseline requirements which **AFB** Business must satisfy in their environments.

The Policy and Standards identify information protection requirements to ensure all Businesses protect **AFB** Information in accordance with applicable global legal and regulatory requirements. The policy and standards represent the minimum requirements for Information Security that all business within **AFB** must follow.

If applicable laws or regulations establish a higher standard than provided here, **AFB** business must comply with those laws. If applicable laws or regulations appear to conflict with the Policy and Standards, the affected **AFB** business unit must inform *CISO*.

The **AFB** Information Security Policy & Standards are a collection of documents and process requirements that must be adhered to by Technology and Businesses in **AFB**. Failure to protect our Information Assets could result in financial loss or loss to our reputation and have a negative impact on **AFB**'s safety and soundness.

The Policy & Standards allow a cost-effective risk-driven approach to manage compliance with our Information Security policies.

Adherence to the Information Security Policy & Standards will help mitigate risks to our information assets while assisting **AFB** in achieving controlled and sustainable growth.

The Information Security Policy and Information Security Standards are aligned with the International Organisation for Standardisation's ISO/IEC 27001 *"Information technology — Security techniques — Information security management systems — Requirements",* ISO/IEC 27002 *"Information technology — Security techniques — Code of practice for information security controls"* and ISO/IEC 27015 *"Information technology — Security techniques — Information security management guidelines for financial services".*

:

1.2 Validity, Scope and Role of these Standards

The security standards are developed based on an internal memorandum / internal circular letter / intranet publication of the IT General Security Policy and apply to Allfunds Bank S.A.U. including its branches, subsidiaries and representative offices (hereinafter together as "**AFB**") and security services associated to the services provided by **AFB** to other Entities of the Group. Likewise, it will always be considered when preparing the security regulations.

There is a transition period to develop the processes and procedures mentioned by *IS Policy & Standards*. This transition period is **6 months** starting from publication date.

1.3 Information Risk Management

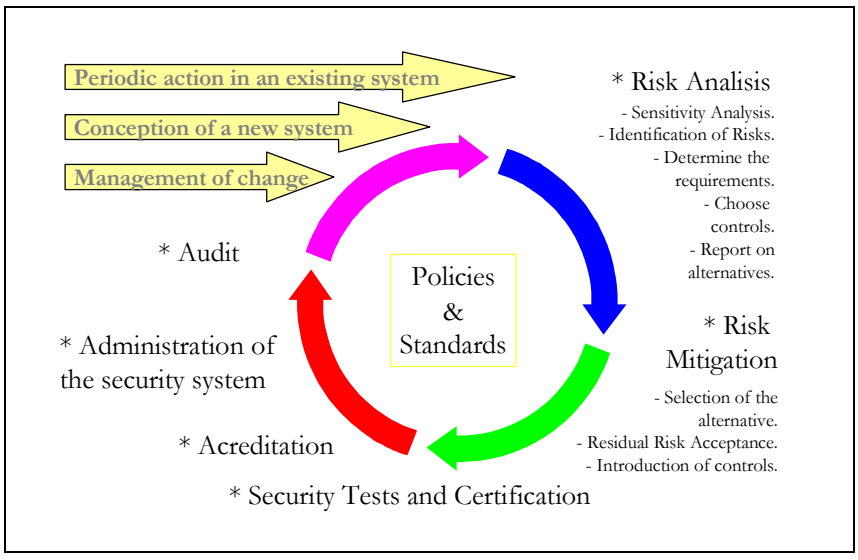
Information is an essential asset for the Group. Any non-authorised loss, alteration, or disclosure of such information can cause loss of business or negatively affect the company objectives. Therefore, information implies some operational risk which is fundamental but not unique to the IT systems.

Technology risk is defined as the risk of loss of information due to the inadequacy or failure of technical infrastructure hardware and software, cyber-attacks, human failure or other circumstances, which may compromise the confidentiality, integrity or availability of information.

At **AFB**, this function is overseen by the IT Risk Management business unit belong to **Risk Management** area, and is therefore governed by a specific methodology for the continuous management of technology risks.

IT risk management involves the identification, measurement, control (preventive, corrective or for detection) and monitoring of risk, to ensure that technology risk is kept at an acceptable level within the risk appetite defined by the Entity. It is also responsible for its communication to the Management.

1.4 Information Security Life Cycle



1.5 Basic Principles of Information Security

1.5.1 Availability

AFB Group personnel must have the necessary information to carry out their work in a precise and timely manner. However, access to data and programs by persons without adequate authorisation will not be tolerated, regardless of whether they are part of the Group. Measures

related to this principle might include Production controls, procedures, back-up copies, physical protection, data recovery systems, and business continuity plans.

1.5.2 Integrity

No action in relation to the **AFB** Group IT environment should cause non-authorised or accidental changes, additions or deletions of information.

1.5.3 Confidentiality

The information owned by the group must only be known by those people who need it to carry out their tasks. Moreover, maximum respect should be given to the privacy of our clients and employees and the disclosure of internal information will be avoided as much as possible. This requirement should be adapted in accordance with the established confidentiality levels.

2 ORGANISATION OF INFORMATION SECURITY

2.1 Roles & Responsibilities

Security policies define the responsibilities of the people who deal with IT data and processes. Any security breach can cause economic losses to **AFB**. Therefore, people related in any way to IT processes must be aware of and understand that **security is everyone's responsibility** and, therefore, everyone must know and apply Group norms in this regard.

As part of the security requirements, it is essential that all employees know their exact responsibilities. The distinct basic levels of responsibilities are defined below. This should be in accordance with the security level, which, in turn, is adjusted in accordance with the inherent risk of the information to be dealt with. Therefore, a classification system must also be established in line with the economic and strategic risk involved. Finally, only an adequate awareness policy will ensure employees' compliance. They should know about risks we take to comply with the regulations.

2.1.1 Top Management

Top Management defines Group IT Security policies, their basic principles, and the objectives to be fulfilled.

2.1.2 IT Security

The position of CISO exists to homogenise and centralise all matters related to **IT Security**.

In **AFB** Group, **IT Security** Management will assume accountability, notwithstanding the existence of a CISO for each existing IT environment in the Group, in Spain as well as in the rest of the world.

Those in charge of security are competent enough to solve all problems related to **IT Security** within the boundaries of their work.

Their responsibilities are as follows:

- Establish the standards, norms and procedures related to **IT Security** based on the Top Management Policies (internal memorandum/internal circular letter) and legal dispositions.
- Collaborate with the Data Custodian in controls defined by the owner.
- Control and establish access mechanisms to the data, processes, and useful tools.
- Evaluate and classify security incidents related to possible information leaks.
- Perform mitigation actions necessary to contain and/or prevent incidents.

2.1.3 Data Owners

The data owner is the business unit's Manager and owns the information stored or processed (Executive in charge).

The Information Owners appointed for each Business must:

- Estimate the information value for **AFB** Group.
- Define criteria for authorising user access to data.
- Implement and monitor security processes under their control to comply with the Information Security Policy and Standards.

- Protect individual assets, establishing an appropriate level of control.
- Information security risk management activities and when an issue is detected, approve the Risk Documentation and make a decision regarding the risk, according to the risk level.
- Verify data controls and modify those deemed unsuitable.
- Authorise the release of information to another entity.

2.1.4 Data Users

"Data User" refers to a person, whether a staff member or collaborator, who, duly authorized, reads, modifies, or transmits information stored in our Information Systems. In order to obtain a user profile, direct or designated authorisation from the Owner is necessary, which can be granted individually or generally (information available for all personnel of an area, for the whole Entity, etc.). The owner can be a user as well and is therefore subject to the same responsibilities.

The Data User's general responsibilities are:

- To use the information only for the authorised purpose.
- Fulfil the controls established in the internal and external regulations.
- Take appropriate measures to avoid disclosure or unauthorised use of information.
- Notify the person responsible of any security problems or data breaches as soon as possible.

Users should only have access to data they are authorised to see or process. Authorisation granted will limit the user's actions in the IT environment such that they cannot carry out any activities other than those which have been approved.

2.1.5 Data Custodians

Data Custodians are personnel or departments which provide all types of IT services in any area of the Group. Custodians do not need data to carry out their work, they are only limited to processing it, managing its storage, and making it accessible. Their responsibilities are:

- To guarantee the setting up and implementation of the controls established by the owner.
- To ensure that access to the data and processes can only be carried out by authorised users.
- Ensure physical protection of the management and data storage.
- To guarantee the fulfilment of the Service Level Agreement (SLA).

They are also responsible for guaranteeing data availability, including in the corresponding Business Continuity Plan.

The IT department of the corresponding business unit is the data custodian of the information system in that business unit. In some cases, other areas and individuals can act as specific data custodians.

2.1.6 Non-AFB Group personnel

Contracts with external companies must include a clause wherein they are obliged to comply with the **AFB** Group IS Policy & Standards and Procedures requirements. Therefore, any breach on their part should allow us to take necessary measures.

2.2 Contact with authorities

No requirements for this section.

2.3 Contact with special interest groups

IT Security will maintain contacts and/or membership with special interest groups and other specialist security forums or professional associations as a way to:

- Confidentially share and exchange information about recent fraudulent and criminal activities.
- Improve knowledge about best practices and stay up to date with relevant security information.
- Ensure that understanding of the information security environment is up to date and complete.
- Gain access to specialist security information.
- Share and exchange information about new technologies, products, threats, or vulnerabilities.

2.4 Information Security in Project Management

Businesses will incorporate an Information Security Review Process (**ISRP**) into their processes and procedures for the selection, development and implementation of applications, products, and services in order to ensure compliance with this *IS Policy & Standards*.

A security review must be documented for each project in which information flows are affected.

This process is under the control of the **IT** area. The *CISO* is part of this process: Information Security participates in the analysis, definition, technical analysis, and UAT phases of application development projects.

2.5 Segregation of Duties

Processes must be put in place to ensure that no individual person can perform any two Business functions or Controlled Information Systems functions with persistent access for the same activity, change, Information System, or transaction without authorisation or detection unless adequate compensating controls are present to mitigate the risk.

There are the following exceptions:

- A Business user may initiate or approve a real transaction and still participate in testing of new requirements for the same Information System in a non-production environment.
- A user with the develop function may provide production support, but persistent access to the production system can only be granted if the access is limited to read or view only.
- A person with the Develop function who needs to provide break/fix support utilising the Implement function must use temporary privileged access to the Controlled Information System.
- A person who needs to update production data outside of application controls must use temporary privileged access in accordance with Access Control section.

3 HUMAN RESOURCES SECURITY

3.1 Prior to employment

3.1.1 Screening

We must ensure that appropriate background checks are performed on all **AFB** staff. This process is completed, directed, and managed as part of **Human Resources** area guidelines for background checks.

3.1.2 Terms and conditions of employment

As permitted by law, Businesses must inform staff who use Information Systems that all communication or information created, sent, received, stored, or processed using these systems or processes is the property of **AFB** and may be recorded, reviewed, monitored, or used by **AFB**, and that staff should not expect privacy in any of their business or non-business use of Information systems.

AFB reserves the right, as permitted by law, to obtain information, including information relating to a worker, from all its systems and processes for administrative, security and other lawful purposes.

3.2 During employment

3.2.1 Management responsibilities

Business Managers must ensure that all employees apply Information Security in accordance with the **AFB** information security Policy and standards.

3.2.2 Information Security Training and Awareness

Businesses must ensure that Information Security awareness materials are distributed to employees annually. **AFB**´s **CISO** is responsible for preparing and promoting Awareness of the Information Security Policy and Standards.

Businesses must ensure that new **AFB** employees receive Information Security awareness on their role and related aspects within **60** days of the job starting. Managers are responsible for ensuring that staff under their control undergo this training.

3.2.3 Clear desk and Clear screen policy

Staff are required to protect sensitive information in all formats, including physical form data used or stored at their workspace.

AFB has put in place a clean desk program that protects all **CONFIDENTIAL** or **HIGHER** information stored on any media from unauthorised access. Details will be included in the **AFB-Information Security and Systems User Manual**. This procedure will be developed and maintained by **IT Security**.

3.2.3. Disciplinary process

Requirements for this section are addressed in the "**General Code of Conduct**" and Human Resources policies and documents.

3.3 Termination or change of employment

3.3.1 Termination or change of employment responsibilities

- User termination from **AFB** must be notified by the **end of the next business day** to the **IT** Team.
- Upon worker termination or transfer to a different job function, all **Functional IDs** owned by or delegated to that individual must be transferred to a new owner/delegate by the original worker's manager or to original worker's manager.
- Managers must review existing user access due to transfers and changes in job functions, within one month of transfer/change or before the addition of new access that may compromise the segregation of duties.

4 ASSET MANAGEMENT

4.1 Asset Liability

4.1.1 Inventory of assets

- Businesses must ensure that an inventory of applications under their control is maintained. IT will oversee that assets inventory.
- IT must ensure that **AFB**'s Infrastructure Inventory of Information Assets is maintained.
- All Functional IDs on Production/Contingency Information Systems must be maintained in one or more inventories, capturing at least the following:
  - ✓ Name of Functional ID.
  - ✓ Brief description or purpose of ID.
  - ✓ Owner of the ID.
  - ✓ Interactive/non-interactive status.
  - ✓ Privileged/non-privileged status.
  - ✓ Password management process/repository.
  - ✓ Entitlement review process.

4.1.2 Ownership of assets

Businesses must designate Information Owners for **AFB** Information under their control.

- Functional IDs on **AFB** managed Production/Contingency Information Systems must be owned, and this owner must be an **AFB** employee.
- The Functional ID owner may nominate one or more delegates to assist in the fulfilment of the responsibilities associated with the ownership of the ID.
- The ID owner is responsible for compliance with all Functional ID requirements.

4.1.3 Acceptable use of assets

- Users are accountable for all activities associated with their login IDs.
- Users are not permitted to access external Internet e-mail accounts from the **AFB** network for non-business purposes.
- The use of remote access to the **AFB** network (over wireless, broadband, dialup, etc.) is not permitted unless the remote connection is made through remote access portal.
- Users must comply with all applicable policies, standards, and guidelines, including **AFB**'s Code of Conduct.

Please, refer to *AFB-Information Security and Systems Use Handbook.*

5 INFORMATION CLASSIFICATION

Diverse criteria exist for classifying information according to distinct aspects. The classifications basically respond to the significance of the data, in terms of its availability, integrity, or confidentiality, establishing a variable number of levels. The current standards establish minimum criteria based on the confidentiality of the information.

In all areas of the **AFB** Group, information classification must be established according to the confidentiality and following important criteria for the business, following the criteria derived from information risk management. (See 0).

The information owner will oversee its classification, although classification review procedures can be established beforehand. The custodians and users will act in accordance with the classification and will comply with the norms established for its access and management.

The impact on the Group that can result from the disclosure, use, modification, or erasure of the information, without the appropriate authorisation, is fundamental to making the classification.

In the case of the co-existence of information of diverse classification levels, the total will be dealt with in accordance with the highest level, except when it is feasible to separate the information by levels in a technically and economically viable way.

5.1 Classification Criteria

For the information stored and/or related to the Entity's systems, the following classification criteria are established:

Level	Description	Impact
Secret	**Highly restricted information** intended for the knowledge of a very small group of people of strategic importance to Allfunds. This is highly sensitive information whose access, disclosure, or modification by unauthorised personnel could cause irreparable damage to the Entity, cast doubt on its credibility as a financial institution, or put the Entity at a disadvantage vis-à-vis its competitors by jeopardising the marketing of products or the Entity's know-how in general. Examples of this type of information may be strategic plans, information on business plans for the launch of new products, internal policies, documents with information on network vulnerabilities, documents with information on security risks to systems and services, etc. Also included in this classification is personal data from special categories. Access to such information is **limited to a very small group of people authorised by the information's owner.**	• High economic losses. • Serious legal violations. • Serious loss of prestige or damage to Allfunds. • Wrong strategic decisions.

Level	Description	Impact
Restricted Confidential	**Sensitive information** whose access, disclosure, or modification may cause significant damage to the Entity, harm its interests, or hinder its mission. Examples of this type of information may be data models, details of system architecture, statistics generated that reflect business activity, studies on differentiation from other entities, information about employees (payroll, seniority, address, etc.) or general information about customers (not financial data) such as their e-mail or telephone number, as well as any type of personal data (not categorised as special). Access to this information is **limited to expressly authorised employees on a need-to-know basis**.	• Moderate economic losses. • Legal violations. • Disrepute or damage to Allfunds. • Taking wrong non-strategic decisions.
Confidential	**Sensitive information** whose access, disclosure, or modification may cause significant damage to the Entity, harm its interests, or hinder its mission. Examples of this type of information include data models, details of system architecture, statistics generated to reflect business activity, corporate policies, and procedures and ISAE reports. This information is **accessible only to employees, as well as to third parties who need access to it for the provision of contracted services.**	• Moderate economic losses. • Legal violations. • Disrepute or damage to Allfunds. • Taking wrong non-strategic decisions.
Internal	Information whose access, disclosure or modification by unauthorised personnel **does not pose any risk to the business or image of the Entity**, however, may be inconvenient for employees or may provide a competitive advantage to other entities to obtain more sensitive information. Examples of this type of information may be organisational charts, internal procedures and methodologies, internal telephone numbers, etc.	• Slight economic losses. • Processes may depend slightly on their accuracy.
Public	Any information not included in any of the above groups and which **does not require any special protection measures.** Information for internal and external use whose loss or unauthorised access does not have a negative impact on the Entity. In this sense, it is information without access restrictions that can be known and consulted by any person.	• It would not cause any harm to Allfunds. • No process depends on its accuracy.

5.2 Crown Jewels

Information considered to be of high value for each of the areas of the Entity whose loss or disclosure could lead to a competitive disadvantage, economic losses, or penalties is called a **crown jewel**. A crown jewel is information that is classified as **Restricted Confidentia**l **or Secret** and must be identified and inventoried by each area of the Entity.

5.3 Security measures

Information shall be protected with security controls and requirements that are proportional to the level of classification identified and applied to such information or information asset.

5.4 Default Security Classification Level

When no explicit reference is made to the security classification of the information, it will be understood that it is Confidential (as most information held by the Entity is confidential), and the necessary security measures must be applied for this type of asset.

5.5 Other Asset Classification

In the same way information is classified, the same will be done with the rest of the assets that treat and/or support it.

Each of the assets will be assigned its corresponding level of classification, which will be based on its importance for the business and the level of classification assigned to it, both the information it contains (if applicable) and other assets that depend on it.

The assigned classification level will be equal to the highest of:

- the level assigned to the information it contains and,
- the assets that depend entirely on it.

5.6 Labelling

The information will be labelled with its classification level, whenever feasible, at the time of its creation (or modification if it affects the previous level). Electronic documents, paper documents and all media containing them shall be labelled, especially when they are distributed.

Where appropriate, an additional label may be applied, indicating the specific scope of information dissemination (e.g., a department, area, division, project staff, building, etc.).

5.7 Assets Reclassification

Whenever substantial modifications are made to certain information, which may imply a change in its classification, the level of confidentiality of the information assets should be reviewed and labelled according to the new status. The time will vary depending on the level of classification. Likewise, the rest of the assets will be labelled with their classification level, whenever they are affected by changes to the information they contain (if any) or to the assets that depend entirely on it.

5.8 Information owned by Third Parties

All information received from non-Group personnel will be treated in accordance with the criteria indicated upon reception. If no indications are received, the criteria established previously must be considered and classified in accordance with the categories in 5.1 chapter.

6 MEDIA HANDLING

6.1 Management of Removable Media

Businesses must protect **AFB** Information regardless of the media on which it is stored. This Policy & Standards applies, but is not limited, to the following types of media on which information is stored: SD cards, USB drives, or other removable storage devices, hard copy output, magnetic disk, magnetic tape, microfilm, microfiche, optical disk, or paper document.

The default setting for access to portable media/storage devices must be **read only**.

6.2 Disposal of Media

AFB information must be protected in accordance with the applicable sections of the *IS Policy & Standards* until it has been destroyed or sanitised. This applies to **AFB** information stored on non-electronic formats (e.g., paper) as well as electronic formats, including but not limited to, digital media/storage devices, files shares, and embedded in office systems such as printers, copiers, or fax machines.

6.2.1 Digital store media

- Digital Media/storage devices that contain **AFB** information must be properly disposed of when they have reached the end of their life or are no longer needed by **AFB**.
- Onsite sanitisation using one of the processes detailed in the sections below must be used to sanitise media.
- Where onsite sanitisation is not feasible, and in case the media must be transported for sanitisation (to the destruction vendor's facility), information asset transfer processes must be documented and followed.
- Where information cannot be successfully wiped using the common solutions/tools, physical destruction should be used.
- A record or log of all destruction or sanitisation activities must be maintained in accordance with the **AFB** Records Management Policy and Standards, by the business or operational unit performing the destruction and include:
    - ✓ Date of destruction/erasure.
    - ✓ Method of destruction/erasure.
    - ✓ Total count of media/drives erased or destroyed.
    - ✓ Person who performs the activities/Vendor name, if applicable.
    - ✓ Type of media (e.g., tape, disk, etc.).
    - ✓ Drive Model/Serial Number (if technically feasible).

6.2.2 Drives (including HD, USB, smartphones, or other units)

a. Mountable, or able to be accessed by erase tool: A tool that randomly overwrites the drive sectors with specific different characters must be used to securely erase mountable media based on the following rules:

- For media that stores **AFB** information, the tool must complete at least five (5) overwrite passes over the media.

b. Unreadable or un-mountable: For Hard Drives that are not readable but with their media intact (e.g., due to a mechanical or circuit level failure), use onsite physical destruction or a secure destruction service provider.

USB ports are disabled by default for copying data in **AFB**. Only EUT Support Administrators and other exceptions upon request have this option enabled.

- To support extract information requests from users:
  - ✓ Authorisations required: Business Unit Director and HR Director. These authorisations will be sent to CIO copying CISO for both authorisations (first CIO and finally CISO).

6.2.3 Physical and other non-electronic records

- Paper and other non-electronic storage media containing confidential or higher Information must be destroyed using specialised external shredding services or using shredder machines.
- Confidential bins must always be locked and may be opened by personnel authorised by General Services (building management), the Business Information Security Office, or a Records Management Department member.

6.2.4 Mobile devices

- Mobile devices that store information that is classified as confidential or higher must be reset by performing a full hard reset as per the manufacturer's specifications.
- Any data exchange between a mobile device and an IT system connected to a group network performed wirelessly (Wireless LAN/IEEE 802.11, Bluetooth, UMTS, LTE etc.) must be encrypted.
- All access from external networks to resources within the Group network is only permitted using a VPN-connection between the mobile device (VPN client) and the VPN gateway.
- If using E-Mail to send confidential, secret, or personal data without using a VPN connection, it must be ensured that PGP or S/MIME with X.509 certificates are used. The user's private PGP Keys must be stored in an encrypted local key store on the device. For S/MIME, the assigned keys must be stored on the smart cards, if possible.

6.2.5 Copies, printers, and fax machines

Copiers, printers, fax machines, and any other device that has persistent memory/storage that may contain confidential or higher information must have their hard drives securely erased or removed as per below:

- copiers, printers, and fax machines must be reset to the factory defaults before being transferred outside of **AFB** premises.
- If leased, it is recommended the vendor securely erases the persistent memory/storage using a process/technique that meets "**NIST SP 800-88** - Guidelines for Media Sanitisation requirements".
- If purchased, the persistent memory/storage must be securely erased/destroyed following the Policy & Standards around media detailed earlier in this document.

6.3 Physical media transfer

- If a cryptographic protection mechanism is not required, the Business must still protect **AFB** Information from unauthorised access, modification, or deletion.
- Confidential or higher Information stored on Electronic Transportable Media (ETM) must comply with the ETM Process with respect to inventory and control requirements

- Encrypted laptops are not subject to ETM inventory and supplemental requirements.
- Hardware elements (servers, laptops, storage devices, smartphones, etc.) and analogue media (microfilm, etc.) are not considered ETM.
- One-time bulk movement of non-portable media/storage devices (e.g., data centre relocations) is not subject to ETM requirements but must comply with general protection requirements.

7 ACCESS CONTROL

7.1 Access Control Business Requirements

7.1.1 Access control policy

AFB must implement access controls that:

- Are fully documented.
- Are auditable.

AFB must protect all Controlled Information Systems from unauthorised access and must secure them using security products, functions, or processes commensurate with the IS Risk Levels of the Information Systems and the Information Classification.

- Each Manager is responsible for the appropriateness and maintenance of the access rights of users under his/her control.
- All user access to Controlled Information Systems must ensure least privilege by the access approver to enforce the most restrictive set of rights/privileges for access needed by users to perform their job.
- Temporary Privileged Access to Controlled Information Systems must follow a documented Technology password/account release process that:
  - ✓ Requires the requester to either be on a pre-approved authorised users list or have approval at the time of use.
  - ✓ Requires documented justification in a change/problem ticket before access is granted.
  - ✓ Includes a process to revoke/remove the access after a pre-defined period of no more than **72** hours.
  - ✓ Allows access to be extended up to **7 calendar days**, for production and post-implementation stabilisation, such as after a major upgrade or break/fix resolution.

7.1.2 Access to networks and network services

- Remote access to Information Systems must be protected from unauthorised use.
- Technology platforms must identify and authenticate peer technology platforms commensurate with the IS Risk Levels of the interaction and other mitigating controls. Where the risk has been otherwise mitigated, no additional authentication may be needed

7.2 Remote terminal access (teleworking)

7.2.1 Basic requirements

For the implementation of a remote access infrastructure the network and server security requirements as well as the hardening requirements must be observed.

7.2.2 User

Remote access to the company network must be approved by management for every individual. The setup, change, and withdrawal of external access rights must be executed via normal user management processes.

Safety and behavioural rules for the internal network also apply for employees with remote access. With the granting of remote access rights, the employee must be advised on security rules for using remote access. Remote access should not be used in public, but if there is a need to do so, all precautions must be taken to preserve AFB information.

7.2.3 Network

Appropriate protective measures must be implemented to ensure service availability for remote access. This includes redundant structures of critical components and the implementation of measures against denial-of-service attacks.

7.2.4 Authentication

There are multiple validations for remote access authentication (user, password, active user in DA and VPN Group).

7.2.5 Encryption/Security of Connection

Connections must be secured with end-to-end-encryption. Only one tunnelling connection at once may be set up per terminal.

7.2.7 Handling of sessions

Automatic locking of inactive sessions must be enforced after no more than 10 minutes.

Connections must be terminated after a fixed time, which should be no more than 12 hours.

7.2.8 Client-Server communication

Besides the allocation of a virtual screen and the forwarding of input data (keyboard and mouse) from the client to the server, only the exchange of the clipboard as well as the integration of local printers is allowed.

VPN connections must be restricted to the minimum necessary.

7.2.9 Logging/Monitoring

All security relevant events must be logged on the servers involved. This includes successful and failed authentication attempts.

Logging of administrative activities must be implemented. Access to these protocols needs to be specially protected.

7.2.10 Documentation of provided environment

Comprehensive documentation must be created for every server configured for remote access.

7.3 User Access Management

7.3.1 User registration and de-registration

A formal user registration and de-registration process should be implemented to enable assignment of access rights by Business. Each group or groups sponsoring a new application must ensure this process is in place.

- All **AFB** technology platforms must authenticate the identity of users or systems accessing these platforms prior to initiating a session or transaction unless the user or system is entitled only to read Internal or Public data on these platforms.
- For all **AFB** managed applications, users must be uniquely identified or mapped to the technology platform by a user ID and Master IDs.
- Access entitlements for all **AFB** managed applications must be traceable to the Master ID.
- Functional ID Owners must ensure processes are implemented which clearly demonstrate accountability for interactive access.
- Remote access to Information Systems must be protected from unauthorised use.
- If a Business permits individual to access **AFB's** network remotely, Business must communicate to each individual that access must be conducted only over approved remote access systems.
- No user can gain access for themselves to a Controlled Information System without approval from their manager (or manager's appointee).
- Persistent Privileged Access may be granted to a user on a Controlled Information System only when all the following conditions are met:
  - ✓ The justification for persistent privileged access is documented as part of the approval.
  - ✓ The user's manager and Controlled Information System owner/delegate approve the access.
- All new Functional IDs or changes to an existing Functional ID on Production/Contingency Information Systems must be approved by the ID owner/delegate and the owner of the Information System on which it resides, as part of the ID creation and/or modification process.
- The Functional ID owner/delegate of any privileged Functional ID must approve additions to the authorised user list, if it exists.
- Requirements for disabling or removing user IDs of users who have left the organisation can be seen in sections *3.3 Termination or Change of Employment* and *7.3.6 Removal or Adjustment of Access Rights.*

7.3.2 User Access provisioning

A formal user access provisioning process should be implemented by Businesses to assign or revoke access rights for all user types to all systems and services.

7.3.3 Management of privileged access rights

- Businesses must implement access controls that ensure users are given only those privileges and entitlements necessary to perform their function.
- Businesses must implement a process to ensure that all default access capabilities are removed, disabled, or protected to prevent their unauthorised use.
- The direct login to a privileged Functional ID must be through a temporary privileged access process.

- An interactive Functional ID on Production/Contingency Information Systems must not be used by the ID owner/delegate.

7.3.4 Management of Secret Authentication information of users

The allocation of secret authentication information should be controlled through a formal management process:

- Users are required to keep the confidentiality of personal secret authentication information when users are required to maintain their own secret information authentication. Initially, they should be provided with secure temporary secret authentication information, which they must change on first use.
- Default vendor secret authentication information should be altered following the installation of systems or software.

7.3.5 Review of user Access rights

Businesses must implement a process (Entitlement Review) to review, verify and delete unnecessary user entitlements.

- Businesses are responsible for the end-to-end entitlement review process around authorisation and access control for all users under their control.
    - ✓ **IT Security** is responsible for the oversight of the entitlement review process, providing support to enable the Business to complete entitlement reviews consistent with documented policies and procedures.
- Business managers may delegate entitlement reviews to individuals who understand job functions/entitlements to be reviewed.
- Business managers/delegates must review user entitlements annually as follows:
    - ✓ All Production/Contingency environments that have an IS risk level of medium, high, or very high must be reviewed at least annually.
    - ✓ All Low IS risk production/Contingency environments unless they have confidential PII or restricted data are exempt from mandatory review.
    - ✓ All Outlook public folders, SharePoint sites and Windows shares/folders (irrespective of information classification of the information stored on them) are exempt from mandatory review.
    - ✓ Non-production Information systems with non-redacted confidential-PII or restricted data must be reviewed at least annually (other non-production Information systems are exempt from mandatory review).
- Business managers/delegates must not review or approve their own entitlements or the entitlements of an individual who delegated review responsibility to them.

The entitlements for all privileged non-fixed Functional IDs on production/Contingency Information Systems must be reviewed annually by the ID owner/delegate.

- The authorised user list for privileged interactive Functional IDs on Production/Contingency Information Systems must be reviewed annually by the ID owner(s)/delegate(s).

7.3.6 Removal or adjustment of Access rights

- Business managers/delegates must request the removal of any unnecessary access through the Information Security Administration function.

- User account termination requests must be processed by disabling user login to desktop/Active Directory, Single Sign-on, email and remote access by the end of the next business day after being notified of the user termination.
- For requests for removal of access not covered by the previous point, access rights must be changed by the security administration function within **3 business days** of being notified of a change.
- Managers must review existing user access due to transfers and changes in job functions within one month of the transfer/change or before the addition of any new access that may compromise segregation of duties.

7.4 User responsibilities

7.4.1 Use of secret authentication information

- User static passwords must never be shared, made known to others, or written down.
- Privileged interactive Functional ID passwords on Production/Contingency Information Systems must not be shared.

7.5 System and application Access control

7.5.1 Information Access restrictions

Requirements for this section are addressed in **IT** procedures.

7.5.2 Secure login procedures

Login IDs associated with a static password must be locked out after not more than **5** consecutive failed login attempts.

- Functional IDs are exempt from the requirement of locking out login IDs after five (**5**) failed login attempts.
- Locked out user login ids must be unlocked through either an IT Support function, or a reset service or an Automatic Soft Unlock out Process.

A banner text, approved by the Legal department for the Business, when supported by the operating system or application, must be displayed at all network entry points where a user initially signs in or is authenticated.

7.5.3 Password Management system

- User static passwords must never be displayed on the screen in clear text.
- Interactive Privileged Functional ID passwords must not be hardcoded in clear text.
- Static passwords (other than PINs) must consist of a minimum of eight **(8)** characters, which must contain both letters and numbers, and be case sensitive. If technically feasible, it should contain special characters**.** Static passwords used by customers are exempt from the case sensitive requirement.
- Functional IDs passwords must consist of a minimum of fifteen (**15**) characters, which must contain both letters and numbers, and be case sensitive. If technically feasible, it should contain special characters.
- Lockout after **5** consecutive failed authentication attempts.

All static passwords must be changed at maximum every **90** days. Static passwords for Functional IDs are exempt from this requirement. Note also:

- Functional IDs can be set to not expire.
- The authentication process, if technically feasible, must ensure that the same password was not used within at least the last twelve (**12**) changes.

Users must be required to re-authenticate after a period of inactivity not exceeding **30** minutes. Activity includes any input to the endpoint (mouse, keyboard, touch screen, etc.). Where enforcement is provided by the password protected screen saver, Application/SSO enforcement is not required.

7.5.4 Selection and changing of password

If the IT system allows it, the changing and selection of passwords must be controlled by the system itself.

The access control systems must permit the changing of passwords by the users each time they deem it necessary.

The initial user password must be immediately changed by the user. Where possible, the system must require that this change should be made. This ensures that the password is only known by the user.

The passwords must not be displayed on the screen in any process in which it is used (connection, usage, etc)

No passwords that are easy to guess will be used. It is strictly prohibited to note down passwords which can be identified by other persons.

The IT system must require the changing of passwords when allowed, up to every 90 days, in accordance with the different confidentiality levels.

The password must not be divulged to anyone and must be changed whenever there is a suspicion that another person knows it.

The passwords of the technicians who start up the computers must be immediately changed after installation.

7.5.4 Use of privileged utility programs

Entities must ensure that the use of Utility Programs that can override system and application controls are restricted and controlled.

7.5.5 Access control to program source code

Requirements for this section are addressed in Technology processes.

8 CRYPTOGRAPHY

The Objective of this section is to ensure proper and effective use of cryptography to protect the confidentiality, authenticity, and/or integrity of information.

The main coding method to preserve confidentiality is encryption. The basic encryption methods to ensure integrity and authenticity are *hash*, message authentication codes (MAC), and digital signature.

Encryption is the most adequate method to ensure the maintenance of the confidentiality and integrity levels required by the companies for protection against the risk of information disclosure.

Data compression is not encryption even if these appear in an illegible format since the message is easily decipherable by anyone with basic coding knowledge.

Information sent to another IT system **must be encrypted** when required for security and/or regulatory reasons.

8.1 Cryptographic controls

This section specifies the types of information and under what conditions information must be encrypted.

8.1.2 Cryptographic techniques selection

Only cryptographic methods whose security and strength has been evaluated and approved by experts may be used, considering the current state of technology, the intended application, and the respective protection periods. In particular, the strength of cryptographic algorithms and a sufficiently large key length must be considered.

In this section, cryptographic algorithms are listed which are considered safe for use within **AFB**. Usage of any other algorithm requires approval according to the exemption process defined in the IT Minimum Standard Exemption Process. Only cryptographic methods which are documented and publicly available for security checks may be used. Furthermore, it must be evaluated whether symmetric, asymmetric, or hybrid encryption techniques are suitable for the intended purpose. For different security objectives, different cryptographic techniques must be used:

Confidentiality:

- Symmetric encryption techniques.
- Asymmetric encryption techniques.
- Hybrid encryption techniques.

Integrity:

- Hash algorithms in order to generate hash values.
- Hash algorithms where a symmetric key is integrated into the calculation, so-called Message Authentication Codes (MACs) can establish integrity.
- Asymmetric signature techniques can establish integrity.

Traceability

- Asymmetric (signature) techniques can guarantee traceability.
- Traceability can be guaranteed using a signature with a valid digital certificate.

There are no cryptographic techniques which directly improve or establish availability. However, if cryptography is used, it is important that availability and responsiveness are not degraded more than necessary.

Symmetric Techniques

- **AES** (Advanced Encryption Standard): FIPS 197 and SP800-38B of the NIST ([NIST, FIPS197], [NIST, SP800-38B]).

Asymmetric Techniques

- **DSA** (Digital Signature Algorithm): ANSI X9.30 ([ANSI, X9.30-1]), FIPS 186-4 ([NIST, FIPS186-4]).
- **ECDSA** (Elliptic Curve Digital Signature Algorithm): ANSI X9.62 ([ANSI, X9.62]), FIPS 186-4 ([NIST, FIPS186-4]), SP 800-57A del NIST ([NIST, SP800-57A]) and SEC 1 of the SECG ([SECG, SEC1]).
- **RSA** (Cryptosystem RSA): ANSI X9.44 ([ANSI, X9.44]), ANSI X9.31 ([ANSI, X9.44]), FIPS 186-4 ([NIST, FIPS186-4]) and PKCS #1 ([RSALab, 2002]).

Hashes

- **SHA-2** (Secure Hash Algorithm): FIPS180-4 ([NIST, FIPS180-4]).
- **SHA-3** (Secure Hash Algorithm): FIPS202 ([NIST, FIPS202]).
- **HMAC** (Hash Message Authentication Code): ANSI X9.71 ([ANSI, X9.71]) and FIPS 198-1 ([NIST, FIPS198- 1]).

https://community.akamai.com/customers/s/article/SSL-TLS-Cipher-Profiles-for-Akamai-Secure-CDNrxdxm?language=en_US

8.1.3 Cryptographic products selection

- According to the protection requirements of the information, certified products and techniques must be used (e.g., by Common Criteria EAL 4+ or FIPS 140-2).
- Functionality and compliance with the specified evaluation level must be guaranteed by independent third-party inspections.
- Independent audits by qualified third parties may also be used to evaluate products. Cryptographic products should be user friendly so that all employees can easily use the encryption software in order to minimise the chance of operating errors and potential compromise.
- During the selection of a product, it must be considered if a software, firmware, or hardware-based component best suits the needs.

8.1.4 Organisational requirements

- Problems, IT Security incidents, or suspected incidents related to cryptographic products must be reported to the appropriate bodies.
- Every user must be informed about the rules for encryption (according to data classification) and reporting channels in case of loss or compromise of keys or authentication media.

8.1.5 Technical requirements

- Prior to commissioning the desired configuration of the cryptographic products (e.g., regarding key length, operating modes, or cryptographic algorithm) must be defined and documented in order to be able to quickly restore it after a system failure or software reinstallation.
- Cryptographic products for users must be pre-configured by the administrator so that the required security level can be achieved without further intervention by the users.
- The cryptographic products must be implemented in a manner that:
  - ✓ users cannot technically circumvent the required basic function.
  - ✓ only the person responsible for the operation can change the configuration.
- Complex cryptographic products require appropriate manuals. Access to cryptographic keys of users must be secured by passwords or PINs.

8.2 Key Management

A key task when using cryptography is management of the corresponding keys. To guarantee safe operation, organisational processes and technical precautions must be implemented. Necessary processes for key management must be documented. Especially, who gains access to which key and how a key can be protected from unauthorised use must be regulated and documented clearly.

8.2.1 Key Generation

Key generation should be carried out in a secure environment using appropriate cryptographic key generators which generate unpredictable, statistically uniformly distributed random sequences while utilising the entire available key space. If user input is used for the key generation it should be difficult to predict.

8.2.2 Key Separation

If possible, cryptographic keys should only be used for a single purpose. Encryption key and signature key should be separated to ensure that the use of the signature key can be linked to a conscious action by the user.

8.2.3 Key Distribution

Key distribution must be secured by measures aligned with the protection requirements (e.g., encryption, personal delivery, Key Management Interoperability Protocol).

8.2.4 Key Installation

During key installation, the authenticity as well as integrity of the key data must be verified.

8.2.5 Key Storage

- Cryptographic keys should be stored in a manner that prevents unauthorised access.
- Systems storing key material must be well protected and access must be limited to a small group of authorised people. The private key must be stored encrypted (e.g., with key encryption key) and should be stored as non-exportable.
- Keys should be regularly backed up to storage locations complying with the requirements detailed above.

8.2.6 Key Archiving and Deposit

- Keys may only be deposited (respectively archived) when the following conditions are met:

- ✓ Access is also required when the original key token is not available (e.g., if an employee leaves the organisation or is absent due to illness).
- ✓ The keys are only used for encryption.

- Apart from that, private keys may never be archived.

8.2.7 Key Exchange

To counter potential compromise, a periodic exchange of keys must be enforced. When introducing the use of cryptographic techniques an exchange frequency must be defined by the organisational unit responsible for operation. The exchange frequency depends on different parameters:

- Type of the device or media (e.g., long-term data storage device, data transmission device)
- Cryptographic algorithm.
- Key length.
- Detection of attacks (e.g., theft or loss of a key).
- Protection requirements of the data.
- Frequency of key usage.
- Volume of the encrypted data.
- Relevant threat potential.
- Security of the key storage.

In case of a key being compromised or compromise is suspected, the organisational unit responsible for operation must immediately exchange the keys. As far as technically possible, all data hosted or stored by the company that is encrypted with the compromised key should be securely deleted and the data should be encrypted with the new key before it is made available again.

8.2.8 Key Revocation

AFB´s staff has the obligation to notify and revoke when the concerned key, or key pair in case of asymmetric keys, has been detected or suspected about its compromise.

A revoked key can, if needed, be reactivated by an administrator so that, in certain cases the key can be used to decrypt data previously encrypted with it, like old backups.

8.2.9 Key Destruction

Keys that are no longer required (e.g., keys after expiration), must be properly revoked. Private keys must be securely deleted after proper revocation. Copies of public or symmetric keys should be deleted, if possible.

In the same way it´s mandatory don´t use same Cryptographic devices in development /test than in production environment.

8.2.10 Protection of keys

Keys must be protected against modification, theft, loss, and destruction. Employees and external partners must properly handle keys they have been issued. Private keys linked to an individual (whether an encryption or signature key) should never be shared. Hardware used for key generation, distribution, storage, and archiving must be protected against unauthorised access, loss, theft, or damage by appropriate security measures (as well as physical security measures).

9 PHYSICAL AND ENVIRONMENT SECURITY

9.1 Secure areas

- Access to any **AFB**'s offices, work areas or secure areas that contain sensitive information will be physically restricted to duly authorised personnel.
- Access to places established as critical (Data Processing Centre or Server Room) will require identification and prior documentary registration. These areas will be duly indicated, and access limited to the personnel responsible for maintenance. If access to them is necessary by unauthorised employees or even external personnel, they must be accompanied every moment by company personnel who have authorised access. Eating, drinking, or smoking within secure areas is prohibited.
- Required offices will be equipped with alarms to monitor any unauthorised physical access.
- Access by external visitors or staff will require identification and registration. While the visitor remains in **AFB** facilities, they must be accompanied or at least controlled, and cannot, in any case, circulate freely.
- Production areas will have the physical security measures necessary to protect the employees and the machines against disaster or external aggression. The Production department itself is responsible for its start-up, maintenance, and compliance. Measures will include physical control of access to guarantee that only persons who must be in the Production area can gain access. Controls will be more demanding in the Computer Room. The security measures must guarantee the security level even when there is no one inside the Production areas.
    - ✓ All visits to the Production area will be recorded.
    - ✓ The computer listings must be monitored to avoid disposing of confidential information. All information of this type must be destroyed beforehand.
    - ✓ The technical and environmental requirements established by the hardware manufacturer and technical teams should be implemented and respected to reduce risks.

Internal staff access outside working hours must be registered.

- All **AFB** staff who have access to Organisation's facilities shall be responsible to maintain and preserve it, as well as to notify any loss or degradation as soon as possible.

<u>Inside Offices</u>

- Any document or paper must be collected from the photocopier, fax, or scanner at the same time after having used said device.
- The shredder should be used whenever it is necessary to eliminate non-public or internal use documentation.

<u>Workplace</u>

- Work equipment must be locked, whenever it is going to be left unattended for periods greater than 15 minutes. For convenience, it will be configured automatically through the domain.
- At the end of the working, day all applications should be closed, user sessions ended, and whenever possible, equipment turned off. If a team needs to do administration tasks, updates... at least the session should always be locked.

- As far as possible, the work environment should be left collected at the end of the day (Clean Desk Policy). This implies that any document or data medium (hard drives, USB drives, papers, etc.) is kept out of sight, keeping locked those that are Confidential or Secret.
- Passwords, usernames, or any other data that could give key information to a third party should not be written anywhere.
- Unless expressly authorised by the *CISO*, it will not be possible to introduce photographs, video, mobile telephones or personal digital agendas that incorporate them into the secure areas defined in **AFB**.

9.2 Equipment Safety

- All equipment and workstations used in business activities, tasks and responsibilities must be physically located in secure areas, out of reach of third parties. It is the responsibility of the person who has this equipment to ensure custody and physical protection during working hours while they are using it. Equipment protection is necessary to reduce unauthorised access to data risk and protect it against possible loss or damage.
- Servers locally deployed in **AFB** facilities supporting the organisation's business processes (application development servers, tests, domain servers, intranet...) must be located in the DC (Data Processing Centre) or server room, being a secure area with added security.
- Users should always follow the manufacturer's specifications when using and maintaining the organisation's equipment and systems.
- **AFB**'s facilities will have adequate power and air conditioning to create a stable and reliable operating environment. DCs have additional controls to ensure the functionality of most critical equipment.

Mobile Equipment use

- Portable equipment must remain tied to a fixed item (i.e., table) when left at **AFB's** or a client's premises or any other place without supervision.
- It is **AFB's** responsibility and its employees (during working hours in which this person is using them) to ensure the availability of these devices, as well as their safekeeping and physical protection.
- Whenever equipment is not being used it should be kept out of the reach of third parties.
- When traveling, the equipment should not be checked-in as luggage and it will always be kept under visual control. In hotels, whenever possible, it will be stored in the safe. In case of loss or theft, contact **IT Security** as soon as possible.
- In case of theft or loss, the loss must be reported to IT Security as soon as possible.

Loss, theft, or equipment breakdown

These events are considered security incidents so could affect the confidentiality, integrity, and availability of the information contained in the equipment. In this case, users should proceed as follows:

- To get the equipment serial number, contact to IT Support.
- Report all facts to the police (hour, place, activity that was being carried out), equipment model, serial number and the company's name and address to which the equipment belongs.

All users are required to report incidents using the notification procedure. **IT Support** should be informed via email as soon as possible. At the same they must indicate:

- ✓ User ID.

- ✓ Place, date, and hour in which the loss or theft occurred.
- ✓ Most accurate possible description of the incident.
- ✓ Classification of the information contained.
- ✓ If possible, impact assessment.
- ✓ Place, date, and time in which the loss or theft occurred.
- ✓ The most accurate possible description of the incident.
- ✓ Classification of the information contained.
- ✓ If possible, an assessment of the impact caused.
- ✓ In case of theft, for all cases police original report must be presented to IT Support.

If written communication is not possible or the incident severity is high, the incident will be communicated by call to **IT Support**. The IT area will temporally block platform access that could be accessed from it.

When the repair of the equipment that stores restricted information requires that it be sent to facilities outside of **AFB** it will be verified that information has been erased. If this is not possible, the storage device containing the information must be encrypted.

Regarding reuse or disposal of equipment, it should always check that sensitive or critical information has been deleted prior to reuse or disposal thereof.

10 OPERATIONS SECURITY

10.1 Operational procedures and responsibilities

10.1.1 Documented Operation Procedures

Requirements for this section are addressed in Technology Processes.

10.1.2 Change Management

All new applications or changes to existing ones must not be transferred to the production area without making sure beforehand that it will not affect nor interrupt the normal processes. It is therefore indispensable to require rigorous compliance with the norms regarding tests, taking special care with programs purchased from outside companies.

All new applications must comply with at least the security standards established at their start-up, being able to require additional measures when the circumstances deem it necessary.

Procedures should allow, when necessary, the return to the situation prior to the start-up of the new program.

10.1.3 Capacity Management

Requirements for this section are addressed in Technology Processes.

10.1.4 Separation of development, testing, and operational environments

- Development environments, test environments, and live IT systems must be separated from each other. Requirements for this separation of environments are addressed in Technology Processes.
- Software is only to be developed and tested in a development and test environment that has been designated for that purpose. It must be ensured that live operation is not negatively affected.
- If possible, tests must be carried out with generated test data (e.g., with a test data generator).
- If individuals are given access to personal, confidential, or secret data that they do not need to fulfil their contractual tasks, the data is to be scrambled in a way that the original data cannot be identified before the data is transferred from the operational system to the test environment.
- The copying or use of information from running IT systems is only permitted with prior authorisation from the information owner. Copied data is subject to the same IT security requirements as the original data.
- After the tests have been performed, information from live IT systems that has been used in the tests must be deleted.
- Access privileges that apply to the live IT systems also apply to the test applications.

10.2 Protection from malware

10.2.1 Controls against malware

AFB must ensure that precautions are taken to prevent and detect the introduction of malicious code (e.g., viruses, worms, trojan horse viruses, adware, or spyware) and must implement preventive, detective, and recovery controls to protect against malicious code.

IT must:

- Implement, update, and maintain technology for anti-virus and anti-spyware on all personal computers on all Local Area Network (LAN) servers, mail servers, and other devices that store content received from external sources.
- Implement an appropriate blocking strategy on network perimeter.
- Implement technical and process controls that provide the capability for blocking access to external Internet email accounts identified as non-business related and present any security information risk.
- Implement perimeter Infrastructure that provides the capability for blocking access to Internet sites that are deemed to be non-business related or present an Information Security risk.

Its configuration must consider at least the activation of the following functionalities:

- ✓ Scanning of incoming email and attached files.
- ✓ Scanning of files when opened.
- ✓ Scanning of programs when executed.
- ✓ Scanning of programs and files downloaded from the internet.
- ✓ Scanning of dynamic content (JavaScript, Applets, ActiveX, etc.), when visualising them with a web browser.

10.3 Backup

10.3.1 Basic Requirements

- Data backups are carried out on several IT systems.
- Restoring of data backup is tested.
- Roles and responsabilities for data backup must be defined and assigned.
- It is identified from which IT systems data backuo is required (IT systems in scope).
- It is defined from which intervals of data backup are required.
- The type of data backup is defined for the IT systems in scope (incremental / full).
- Frequency and type of backups must be defined and aligned with the organization's business requirements (Service Level Agreement, where appropriate Business Impact Analysis or Protection Needs Analysis).
- It is checked if data backup was successfully carried out.
- Data backups must be stored separetly from the IT system in a different fire compartment.
- The reliability and usability of data backups is regulartly tested following defined test schedules.
- Access to data backup is permitted only for authorized persons.
- Backup media is adequately labelled.
- Backup restoration procedures are carried out on a regular basis.
- Immediate access to data backup is ensured in case of emergency.
- A data backup guideline is documented and made available to involved persons.
- Backup concepts for IT systems in scope are documented and made available to involved persons.
- Process owners regularly check compliance with the regulations for data backup.
- Corrective measures derived from the compliance checks are carried out.

10.3.2 Storage Requirements

- The backups are stored in different locations:
  - ✓ Backup in cabin replicated in Yécora and Torrejón. Asynchronous copy.
  - ✓ Third copy in cloud, monthly and annual.
- Cloud copies are stored in the IBM Cloud eu-de Region.
- The execution of the Backup and Restore tasks is carried out according to the IBM guidelines for TSM.
- The details of data retention will be explained in more detail in a separate section.

10.3.3 Protecting Backups

- Backups must be protected against unauthorised access.
- It must be ensured through access control that only responsible backup administrators can access the backups.
- Only customised user accounts must be used. Technical user accounts may only be allowed if the user can be identified.
- Separation of roles for backup administrators is must be implanted.
- Backups must be protected against physical and environmental influences.
- Backup media must be stored separately from the IT system in a different fire compartment. Depending on the security classification, offsite backups must be stored in a different location/site at a suitable distance from the backup system.
- Backup media should be handled according to the manufacturer's specifications.
- The maximum recommended lifetime of the backup media should also be observed.
- Copies should remain encrypted, either at cabin or data level.
- All critical systems must have a third copy located outside the DCs.

10.3.4 Backup Retention

The backup schedule is aligned to the business requirements for information recovery and data retention. Backup jobs are monitored by dedicated individuals or a team. Backups are regularly verified, and failed jobs are rescheduled retrospectively as part of routine IT health checks.

- Backup daily incremental 7 days retention.
- Weekly full 4 weeks retention.
- Monthly full 13 months retention.
- Annual full 10 years retention.

10.3.5 Deletion of Back-up Information

When confidential information is to be eliminated, the external storage support must be destroyed, if possible, otherwise it must be deleted in such a way that the information cannot be recovered by any means.

10.4 Logging and Monitoring

10.4.1 Event Logging

All transactions must be logged, in such a way that the origin can be identified, when the system allows it, the audit trails must be registered which permits the verification of the system

integrity, the proper information distribution and the log of all activity to be controlled after the event.

Events as describes:

- Infrastructure security relevant actions.
- All system alarms associated with a firewall or other perimeter Security element generating Security event must be logged.
- All attempted violations of system security (e.g., failed user login attempts) must be logged.
- All significant events relating to financial transactions and customer information which specifically include the following items must be logged:
  - ✓ Updates to financial transactions.
  - ✓ Updates to Confidential PII data.
  - ✓ Updates to Restricted data.
  - ✓ Updates to Authentication data.
- Session artifacts (IP address at minimum or other pertinent information, such as a unique device ID) must be captured, if technically feasible, and logged for customer facing applications (web sites and mobile applications) to support Fraud investigations. These artifacts must be captured for customer transactions and for customer account opening activity. Information must be captured in such a way that the session artifact can be linked to the transaction or account opening.
- Significant Security Administration events must be logged: specifically including the following items:
  - ✓ User creation.
  - ✓ Modification of user access rights.
  - ✓ Deletion, creation, and modification of roles/profiles on the Controlled Information System.
  - ✓ Password reset.
  - ✓ Changes to system security configuration.
- All interactive activity of privileged Functional IDs must be logged.
- Security logs must contain at least the following information regardless of the system generating the log unless it is not technically feasible:
  - ✓ Date and time of the event.
  - ✓ User ID of the person performing the action.
  - ✓ Type of event.
  - ✓ Asset or resource name affected.
  - ✓ Type of access (delete, modify, etc.).
  - ✓ Success or failure of the event.
  - ✓ Source (terminal, port, location, IP, Hostname, etc.).

10.4.2 Protection of log information

- There must be controls in place to preserve the integrity of audit trails:
  - ✓ During initiation and shutdown.
  - ✓ In storage and during transmission.
- There must be controls to avoid logs be overwritten or modified by system users whose activity they track based on log risk.

10.4.3 Outside Personnel Activities

The access and activities carried out by non-Group personnel will be specially monitored in the audit trail processes. Their activities will be logged and revised with special attention.

10.4.4 Clock synchronisation

All relevant information's clocks processing systems within an organisation or security domain must be synchronised with an agreed accurate time source (NTP).

10.4.5 Information systems audit considerations

- Most logs are captured for forensic purpose only,
- Technology processes will provide details about logs that must be reviewed either directly or through an automated review process.

10.5 Control of operational software

10.5.1 Installation of software on operational systems

Detailed requirements for this section are addressed in Technology Processes.

Management must ensure that:

- Only operating systems and software that are currently supported by an approved vendor or have an active and appropriate release of patches and configuration updates available to address security issues are used.
- There must be a process based on risk to evaluate the security patches, to test and apply them. This process will have into account the risk of the vulnerability and the risk of applying the patch to decide when each security patch must be applied.

Application Managers must ensure that **AFB** software developed internally or externally and made available for external distribution or use:

- is maintained so as not to require use of versions of non-**AFB** supporting software with known vulnerabilities. When vulnerabilities in non-**AFB** supported software are reported (e.g., Qualys, Nessus…), **AFB** area that develops software (IT or Digital mainly) must work with patched/remediated version of such supported software in accordance with the Vulnerability Threat Management process.
- is properly updated and patched.

10.6 Technical Vulnerability Management

10.6.1 Vulnerability Framework

- Our entity must ensure that all **AFB** products, services, applications, and associated content follow same management process and have any vulnerability issues remediated within the timeframes described in ***Allfunds- Vulnerability Framework***.
- Managers of technology Infrastructures must ensure that Vulnerability Assessments of their technical Infrastructure are performed in accordance with this related framework.

10.6.2 Restrictions on software installation

- By default, users cannot be machine's administrator, so all the software installation must be done by the **IT Support Team**.

- Any new software or hardware required will be requested to Technology and will be analysed and approved/rejected for **IT Security**.

11 COMMUNICATIONS SECURITY

11.1 Network Security Management

11.1.1 Global Requirements

- Networks must be protected from threats and Network components must be centrally administrated.
- Documentation must be up to date.
- Access to network components must be authenticated and logged.
- Network components must be hardened by disabling unneeded services.
- Network components must be secured appropriately regarding load driven offences like DoS, DDos.
- Management of network components must use secure protocols (e.g., SSH-2, TLS 1.2, SNMPv3.
- All **AFB** external network connections must be authorised by **IT Security**.
- Information with a confidential or higher classification must not be persistently stored on a system in an Internet-facing Demilitarised Zone (**DMZ**). Technology must ensure that:
  - ✓ All Internet connections to the **AFB** network are terminated in a managed network monitored by a real-time Intrusion Detection System (**IDS**), Intrusion Prevention System (**IPS**) or similar perimetral protection.
  - ✓ Non-Internet connections for Third Parties (e.g., B2B) to **AFB**'s network is monitored by Network visibility and threat detection tools.
  - ✓ All **AFB** managed Internet connections that carry production traffic are protected by an **anti-DDoS** (Distributed Denial of Service) and **WAF** (Web-application firewall) service for attack detection and mitigation.
- External firewalls must be configured with a default "**deny all**" rule with all configurations.
- All firewall rules must be configured based on the **least privilege** principle unless the risk of principle violation is insignificant.
- There must be additional telecommunication resources as backing that permit their use in the event of possible incidents (line breakdown, transmission equipment, etc).

11.1.2 Security of network services

- Security components used shall protect **AFB**´s network against potential internal risks (e.g., through employees).
- The structure shall be designed in such a way that possible damage scenarios are prevented.
- It must be ensured, that it is not possible to access protected services via authorised access to another service.
- Network activities shall be traceable (e.g., through network access logs and retention in compliance with logging policy).
- All Services should be protected by appropriate encryption (e.g., TLS 1.2 (https), SSH-2, STFP…).
- Each system must be integrated into a protection requirement class according to a directive. As a result, the system must be incorporated into the zone concept of a suitable

zone with adequate protection mechanisms. No system may be put into service without classification. A regulation for the classification of systems in zones must be defined.

11.1.3 Segregation in networks

Management must ensure that Information Systems are segregated on **AFB's** network in accordance with the following controls:

- Applications accessible to the Internet must be accessed via DMZs.
- **AFB** hosts that permit access by Third Parties must have containment controls in place in accordance with IT processes.
- During an emergency event, management must be able to filter access between portions of the network to reduce the impact from network Security Events (e.g., port filtering during a virus outbreak).

11.2 Network Access

A network access control (NAC) solution based on **internal certificates** must be implemented to authenticate devices connecting to the office network.

11.2.1 Authentication

- NAC must be operated in the access area of the network, i.e., on the level of network ports dedicated to endpoint connections within the LAN.
- Device authentication must be used.
- End devices should be authenticated with a certificate.

11.2.2 Authorisation

Authorisation must be carried out based on the authentication result by assigning the end device to one network access rule:

- End devices that authenticate with certificate must be assigned to the trusted access rule providing an unrestricted communication for the device group.
- End devices that do not authenticate via certificate, but are authenticated based on their MAC address, must be assigned to a restricted access rule, providing only restricted communication.
- End devices that do not authenticate or do not successfully authenticate will have their connection terminated.

11.2.3 Revocation and emergency procedures

- Techniques to explicitly deny devices from accessing the network must be implemented.
- Emergency procedures to disable network access control (NAC) must be provided.
- Disabling network access control functionalities in case of an emergency/failure must follow defined escalation procedures and define permissible actions.
- Procedures to allow temporary network access for unauthenticated devices should be implemented.

11.2.4 Wireless LAN (WLAN)

- These devices should always have access controls at the same level of controls required for wired networks (All requirements of the wired LAN apply to the WLAN).
- The connection of the wireless devices, such as WiFi or Bluetooth to **AFB** wireless connection will use safe communication protocols that prevent its interception and reading by a third party as well as the connection of an unauthorised third party to the company wireless network.
- The wireless devices should have access control which would prevent their utilisation by non-authorised third parties in the event of theft or loss.

Recommended protocol

- **WPA2-PSK (AES)**: the latest Wi-Fi encryption standard, and the latest AES encryption protocol. Except for very justified exceptions it should be our only option.

11.2.5 Guest Access

- Internet connection for guests by the WLAN infrastructure may be offered.
  - ✓ Guest network must be physically separated from the internal networks.
  - ✓ Communication between the guest network and internal network is forbidden.
  - ✓ Communication between guest computers is forbidden.

11.2.6 Remote access and virtual private network

Remote Access and VPN are possible methods for accessing **AFB**. They can be used by both **AFB** staff and staff of contractual partners (e.g., for maintenance). Both communication techniques imply that the communication partner cannot be clearly identified when setting up a connection.

- Multiple validations for remote access authentication (user, password, active user in DA and VPN Group) are deployed.
- Encryption to ensure confidential handling of the transmitted information and integrity of the communication channel.
- The access of the communication partner must be restricted to the target system and to the required services.
- All steps of the communication partner should be logged and monitored if the communication partner needs administrative access for a system.

11.3 Information transfer

11.3.1 Information transfer policies and procedures

The transfer of information must be done while protecting the information according to its classification and following the *Cryptographic controls* in chapter 8.1.

In order to guarantee proper functioning and maintenance, it is essential to continuously document the status of the network. Particularly, detailed documentation will be kept at the disposal of the persons in charge of security and maintenance with Group confidential information security level:

- Diagram and network description.
- Description of all equipment.
- Details of equipment changes.
- Description of access, security, and control points.

- Backup and recuperation procedures.
- Logging incidents in Group IT areas and reporting on them.
- Preventive network maintenance.

11.3.2 Agreements on Information transfer

Agreements should address the secure transfer of business information between the organisation and external parties.

11.3.3 Message Protection

Since it is impossible to base security exclusively for physical measures, security measures will, mostly cases, be logical and will be used in accordance with necessary security level. Among the accepted measures for these standards are:

- Encryption to assure data confidentiality and integrity.
- Authentication to ensure its integrity.
- Identification of terminal.
- Limited user or terminal access.
- Data or time terminal access restrictions.
- Time stamping.
- Digital Signature.
- Inclusion of data control in messages.

11.3.4 Confidentiality or non-disclosure agreements

AFB staff must not, either directly or indirectly, transfer any confidential information to any person, except for personnel of the company or of its suppliers who may need to know such information to perform the functions for which they have been engaged, as long as they have signed a Non-disclosure Agreement (NDA).

12 SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

12.1 Security requirements of information systems

12.1.1 Information security requirements analysis and specification

The security requirements for an application need to be captured and evaluated. Here, requirements for the technical implementation as well as functional requirements (e.g., "transactions have to be protected with a two-factor-authentication") come into effect.

The following questions should be answered at least:

- Who will use the application?
- Which security requirements do the users have?
- Which security requirements does the future software operator have?
- Which data are processed in the application and which protection need do they have?
- In which environment (In-house/external, Intranet/Internet, security zone, etc.) will the application be operated?
- Which availability requirements for the application do exist? What failure is acceptable?
- Who are potential attackers and what motivation do they have?
- What could be potential attack points/vulnerabilities?

Appropriate principles and decisions for the application design must be derived from the security requirements analysis.

12.1.2 Securing application services on public networks

It is vital to know the information type and under what conditions information must be encrypted or otherwise cryptographically protected encryption solutions.

12.1.3 Protecting application services transactions

Information involved in application service transactions is protected by using algorithms recognised by the Industry incorporated into the products implemented.

12.2 Principles

12.2.1 "Minimal Trust" Principle

When processing data, it always must be considered that the data could come from an attacker. Any input data must be checked. This check is necessary for all data accepted by the application. That means it is also necessary for technical data which do not come from a user (e. g. data from HTTP-Header in web applications).

12.2.2 "Least Privilege" Principle

Rights of users and system components always must be assigned according to the minimum principle. A user is only allowed to execute those actions necessary for his tasks/role; same applies to system services and components. Hereby, the possible damage caused by an attacker during the takeover of a user account/system should be minimised.

12.2.3 "Defence in Depth" Principle

As the vulnerabilities in applications can never be avoided completely, a multistage defence against attacks needs to be implemented. The basis for this is the implementation of applications in a multilayer architecture which especially provides a separation between application layer/business logic and data repository. In the case of external reachable applications, at least a 3-level network architecture (see network zone concept) needs to be supported.

In addition, data must be validated again within down streamed processes/systems – it should not be assumed that the delivering systems always forward valid data. It must be especially assured that an action really was initiated by the specified user.

12.2 Security in development and support processes

12.2.1 Secure development policy

IT Security must be part of early phases of software development projects and when Information Security can be affected, during all the process for acquisition, development, and maintenance of software.

The *CISO* must be involved from early phases of the theses processes. This will be detailed in **IT processes**.

12.2.2 System change control procedures

Changes to systems within development lifecycle should be controlled using IT processes.

12.2.3 Technical review of applications after operating platform changes

Technical applications review after operating platform changes should be controlled by IT processes.

12.2.4 Restrictions on changes to software packages

In some cases, development can be avoided by the purchase of external programs which would require little or no adaptation to our IT needs. The security level of these applications (hereinafter "IT Packages" or "Packages") must be assessed before their purchase, considering controls already established within. The code must be revised in sensitive applications.

12.2.5 Secure system engineering principles

- **Input validation:** the following order should be met:
  - ✓ Adjustment of the data (encoding, removal of not permitted signs, etc.)
  - ✓ Normalisation of the data (e. g. removal of „/../" within path specifications)
  - ✓ Validation of data content:
    1. Type.
    2. Data length.
    3. Forma.
    4. Allowed value range.

Blacklisting (filtering of certain unwished values) should basically be avoided. Whenever possible, a **whitelisting** (only allow permitted values) of data values should be implemented.

If the review of login data has a negative result, the data must be rejected. The application must not try to "repair" the data.

- **Processing of data:** different methods can be used, e.g.:
  - ✓ Formation of checksums.
  - ✓ Re-validation of data.
  - ✓ Logical review of data (adherence of limits, etc.).

- **Output control:** this especially applies to special characters included in the data or problems which result from encodings. Different target systems as databases, XML-Interpreter or browser interpret miscellaneous non-alphanumeric characters as metadata or control characters.

- **Separation of program logic and data:** program logic and data must be separated within the source code to impede a manipulation of the program sequence through infiltration of malicious data.

- **Handling of errors:** application user must never be shown details about an error (version number, technical error messages, debug messages, stack traces, path specifications, etc.), as this information could be used against an application by an attacker.

13 SUPPLIER RELATIONSHIPS

13.1 Information security in supplier relationships

13.1.1 Information security policy for supplier relationships

- Businesses must maintain appropriate security of **AFB** Information and Information Systems that are accessed, processed, disposed, or managed by Third Parties.
  - ✓ When establishing or expanding **AFB**'s relationship with a third party that will host an **AFB** branded Internet facing application or be given access to **AFB** Confidential or higher information, Business must complete a Third-Party Information Security Assessment in accordance with Security standard process. Assessment will be leaded by CISO with the Relationship manager's support.
  - ✓ For all Third Parties in scope, an assessment must be completed within the determined timeframe.
  - ✓ Businesses utilising third parties that make use of subcontractors (4th parties) that access, process, manage or dispose of **AFB** confidential or higher information as outside of the Third Party's facilities and/or direct management control must evaluate the information security oversight and controls that these third parties have over their subcontractors (as specifically assessed within Third Party process subcontractor section).
- Businesses must follow ***Allfunds- Vulnerability Framework*** to ensure that vulnerability assessments are performed.
- Businesses must notify IT Security if they receive notification from a Third Party of any unauthorised access or acquisition of **AFB** Information, or any compromise to Information Systems used to store, process, or transmit **AFB** Information.

13.1.2 Addressing security within supplier agreements

- Agreements with Third Parties, which provide application services (i.e., off-the-shelf and custom) as part of business relationship must include the right to periodically perform an independent Vulnerability Assessment, in accordance with ***Allfunds- Vulnerability Framework***.
- All Third Parties agreements who are in **AFB**'s scope must include:
  - ✓ Right to periodically perform Security assessments.
  - ✓ The Third Party must notify to **AFB** Business when there has been any unauthorised access or any compromise to Information Systems used to store, process or transmit **AFB**'s information.
  - ✓ Requirements that Third Party performs all reasonable efforts to return or destroy all **AFB** Information during or at the end of the agreement.
  - ✓ Third Party must notify **AFB** about subcontractors use who will be given access to **AFB** information with confidential or higher information classification; as well as the right for **AFB** to approve the subcontractors.

13.1.3 Information and communication technology supply chain

No requirements for this section.

13.2 Supplier service delivery management

13.2.1 Monitoring and review of supplier services

Business must ensure that Third Parties (excluding customers accessing their own information) that storing, processing, managing, or accessing of **AFB's** Information (except internal and public Information), host **AFB** branded Internet facing applications, or have connectivity to **AFB**'s network resources comply with applicable sections of ***Information Security Policy & Standards*** or provide equivalent controls. It will be done in accordance with Third Party Security Process.

13.2.2 Managing changes to supplier services

- External network connectivity that provides Third Party access to **AFB** resources requires management to ensure, either annually or when Third Party status or access has changed, that the access accurately reflects current Third-Party relationship status.
- Business requesting Third Party network connection is responsible for maintaining information regarding Third Party relationship, including legal contracts, and communicating material changes **AFB** Infrastructure provider's relationship.
- **AFB** Infrastructure providers are responsible for maintaining information regarding connection technical implementation and linking this to the relationship information provided by the Business responsible for Third Party network connection.

13.2.3 Secure development environment

IT should assess risks associated with individual system development efforts and establish secure development environments for specific system development efforts, considering:

- Data sensitivity to be processed, stored, or transmitted by system.
- Applicable external and internal requirements (e.g., regulations or policies).
- Security controls already implemented by the organisation that support system development.
- Trustworthiness of personnel working in the environment.
- Degree of outsourcing associated with system development.
- Need for segregation between different development environments.
- Control of access to the development environment.
- Environment Change monitoring and code stored therein.
- Backups are stored at secure offsite locations.
- Data transfer control.

13.2.4 Outsourced development

AFB supervises and monitors outsourced system development activity across the project lifecycle.

13.2.5 System security testing

Security functionality testing should be carried out during development following **IT** Processes.

13.2.6 System acceptance testing

System acceptance testing should be carried out following IT Processes.

13.3 Data Test

13.3.1 Data test Protection

It is not permitted to put confidential-PII, Restricted, or production authentication data on a Non-production system unless one of the following requirements is met:

- ✓ The data has been irreversibly redacted, so the sensitive information cannot be associated to the right person. Some methods can be used: scrambling, obfuscating, masking information, etc. OR
- ✓ The Non-Production System is subject to the same controls as the production system, OR
- ✓ An exception is documented and approved explaining the reason, the affected applications, the compensating controls, and it is approved by BISO and the Information or Process Owner.

The copying to or from, or the use of this data on a Non-Production Information system must be approved by **IT Security** or **Process Owner** as part of a documented approval process that includes the delineation and implementation of specific controls needed over access to this data (e.g., redaction). This can be accomplished using a one-time approval process that must be renewed if additional fields have been added that would require redaction.

14 INFORMATION SECURITY INCIDENT MANAGEMENT

14.1 Management of information security incidents and improvements

14.1.1 Responsibilities and procedures

- Management must ensure an effective approach is applied to Information Security incidents management and that complies with the SIRT process.
- When a Security Events occurs, a SIRT response must be generated and escalated through the defined SIRT Process.

14.1.2 Reporting information security events

- The following information security incidents, events and vulnerabilities must be reported as follows:
  a. Suspected viruses and/or malicious code must be reported immediately to an individual's or group's designated help desk or support structure.
     - ✓ Confirmed Trojan Horse viruses must be treated as IS incidents.
     - ✓ Viruses that cause a denial of service or are specifically targeted at **AFB** must be treated as IS incidents.
     - ✓ Viruses that appear to affect multiple machines must be reported to the Security Operations Centre (SOC).

  b. Suspected phishing events may be reported to an individual's or group's designated help desk or support structure.

- Customer-facing organisations must have and must communicate a process to their customers to report security related events.
- Any suspicious activity must be acted upon immediately.

14.1.3 Reporting information security weaknesses

The following information security incidents events and vulnerabilities must be reported as follows:

- Application vulnerabilities must be reported to **IT Security**.
- Infrastructure vulnerabilities must be reported to **IT Security** and **IT Infrastructure** team.

14.1.4 Assessment of and decision on information security events

Requirements for this section are addressed in *Allfunds_Security Incident Management Handbook*.

14.1.5 Response to information security incidents

Requirements for this section are addressed in *Allfunds_Security Incident Management Handbook*.

14.1.6 Learning from information security incidents

Requirements for this section are addressed in *Allfunds_Security Incident Management Handbook.*

14.1.7 Collection of evidence

Requirements for this section are addressed in *Allfunds_Security Incident Management Handbook*.

15 BUSINESS CONTINUITY MANAGEMENT

15.1 Framework and Principles

The continuity of Business program is designed to safeguard **AFB** staff, business operations, and technology under a diverse set of conditions, including a resolution event.

The Business Continuity Plan (**BCP**) provides a governance framework for crisis management and the orderly restoration of business activities upon the occurrence of an adverse event (e.g., a natural or man-made disaster or technological failure).

Technological Contingency Plan (**DRP**) must be in place to determine which actions to take after the incident, depending on its magnitude, as well as to anticipate alternative work resources during the time needed to recuperate and establish the procedure of restoring IT equipment and processes in the shortest time possible, based on a previously analysed cost benefit. It will cover both the IT resources as well as all others involved in the work in general: personnel, premises, data, telecommunications, etc.

Both Plans must establish policies and procedures aimed at its periodic updating, testing and maintenance. Periodic testing will serve to detect possible deviations or errors, to adapt or improve Plans and ensure success.

It is based on the following principles:

- First premise and priority objective are personnel´s protection and safety, both in normal and contingency situations.
- It will protect **AFB's** reputation and sustainable development.
- **AFB**'s Management will be responsible for processes considered critical to managing key risks for operational continuity.
- **AFB** will ensure that business continuity plans are in place, considering all areas, and critical service providers.
- **AFB** will ensure that all Business and Support Areas staff are informed of their responsibilities within the Business Continuity framework, through periodic training, awareness and testing of Business Continuity Plans.
- **AFB** ensure that critical processes are recovered within the time frames required by the Business Continuity Plans.
- Management will guarantee Business Continuity capacity within the company culture, as well as Business Continuity Plans impacts in new developments of AFB.
- **AFB** will ensure the existence of dialogue´s channels with different stakeholders to find out their expectations and needs, transmitting their commitments and appropriate communication plans preparation, both internal and external, which will be reviewed and updated periodically.
- **AFB** will ensure compliance with existing regulatory system during development of contingency and recovery activities.
- **AFB** will ensure compliance with current legislation and contractual commitments.

All the detailed data is included in the *AFB-Business Continuity Handbook.*

15.2 Business Risk and Impact Analysis (BIA)

BIA questionnaire (Business Impact Analysis) aims to identify critical business units, its financial, legal, and reputational impacts, recovery time objectives, key personnel, essential suppliers, and information systems among other data considered critical within the Business Continuity Plan.

BIA is completed by each **AFB** business unit. In major Contingency event (disaster or loss), the BCP Leader would activate, within the established deadlines, critical services identified in the BIA Questionnaire.

In each BIA, a Responsible is identified, a Business Unit Coordinator and a Backup Coordinator, completing contact phones, emails, etc. as well as other general information about the team involved, such as number of internal/external staff, personnel by location, etc.

The recovery strategy is built from these two elements (disaster/probability and business/critical processes).

15.2 Risk Analysis (R.A.)

It is **AFB**'s Risk Management responsibility to carry out a continuous improvement of this process in order to respond to attack vectors evolution and ensuring those controls inclusion that mitigate risks arising within **AFB** or industry.

15.3 Crisis Management

Crisis Management will implement adequate plans to the possible contingency scenarios previously identified.

This Management must be able to apply strategies, measures, plans, and resources necessary to act in unforeseen events that could have negative impacts on **AFB**'s business objectives in economic, operational, reputational or social terms.

Crisis management teams and appropriate Crisis management tasks and severity are defined in *AFB-Business Continuity Handbook*.

The crisis management plan is included in the *AFB-Business Continuity Handbook* and contains the CoB site procedure activation, Command Post and Crisis Management team details.

15.3.1 Crisis Committee components

COMMITTEE ROLE	CALL AS...	TITLE AND NAME
Crisis Leader	Head Member	**General Director** Juán Alcaraz López: jalcaraz@allfunds.com
	Head Member	Gian Luca Rencini: grenzini@allfunds.com
Crisis Coordinator	Head Member	**CISO** Javier Torres Alonso: javier.torres@allfunds.com
	Backup	**Business Continuity Coordinator** David Aguado Calle: david.aguado@allfunds.com

Legal Area Responsible	Head Member/ Secretary	**Global Head of Legal** Marta Oñoro Carrascal: MOC@allfunds.com
	Backup	Gonzalo de Sala Ribe: gdesala@allfunds.com
IT Area Responsible	Head Member	**Global Head of IT** Mariano Blanchard: mariano.blanchard@allfunds.com
	Backup	Enrique Martín Roldán: enrique.martin@allfunds.com
Operations Area Responsible	Head Member	**Global Head of Trading & Execution** Francisco Morón Torres: frmoron@allfunds.com
	Backup	Raúl García García-Izquierdo:raul.garcia@allfunds.com
Communication Area Responsible	Head Member	**Global Head of Communication** Katherine Sloan: katherine.sloan@allfunds.com
	Backup	Leticia Labernia Carbajal: leticia.labernia@ext.allfunds.com
HR Area Responsible	Head Member	**Global Head of HR and Facilities** Jorge Calviño Pérez: jorge.calvino@allfunds.com
	Backup	Ofelia Nieto Rodríguez**:** ofelia.nieto@allfunds.com
Risk Management Area Responsible	Head Member	**Global Head of Risk Management** Abraham Magán Delgado: abmagan@allfunds.com
	Backup	Alejandra de las Heras Cabeza: alejandra.lasheras@allfunds.com
Corporate Finance Area Responsible	Head Member	**Global Head of Corporate Finance** Amaury Dauge: amaury.dauge@allfunds.com
	Backup	Alvaro Perera Peña: alvaro.perera@allfunds.com

15.4 Plan Development

BCP must allow for a clear definition of the actions to take before, during, and after contingency. A great number of scenarios are possible, depending on contingency or operation discontinuity root causes as well as business impact levels.

- The Plan must be based on business-critical processes restoration, time windows and user-defined service levels (minimum needs). It must contemplate everything from mere data losses up to full disaster level which would require alternative site. Plan will indicate alternative centre when this will be as solution.
- This rating must be obtained from the Business Impact Analysis (BIA) and corroborated by periodic Plan Testing.

- Once the Crisis stage is over, the Plan will contain policies and procedures to go back to business as usual.
- The Plan can be kept on paper copies or in a printable format. Copies will be kept externally in storage in the alternative centre to avoid its destruction during disasters.
- All personnel affected by the Plan should have a detailed copy of the activity they have to carry out in the event of an emergency.
- The Business Continuity Plan should be updated on a regular basis (yearly) or when circumstances change. The document must be updated.
- There should be copies of each activity stored externally so that a new copy can be provided in case they are misplaced.

15.5 Management Commitment

Through this Policy, Top Management expresses its support and commitment to Business Continuity activities, explicitly declaring its knowledge and approval of this policy so that all staff (internal or external) must know and apply it according to their own roles and responsibilities as part of the Company.

15.6 Third Party providers (suppliers)

For **AFB** suppliers that operate, perform, or manage all or a significant part of a critical business function, especially those who are essential, it is necessary to verify that, in case of a contingency, these vendors have continuity of business plans that include the critical services provided to our entity. **AFB** must take a proactive role and consult with the respective supplier to understand the supplier's COB Plans affecting **AFB** services.

These critical vendors must have documented business continuity plans to ensure that any interruption with respect to the products and services the Supplier provides to **AFB** are addressed and corrected within **AFB**'s defined recovery timeframes. The vendor should be able to show the documentation they have in place (on the vendor's premises).

15.7 Awareness and Training

IT Security manages a Corporate Training and Awareness Program for all staff.

15.7.1 Awareness

Every year, **IT Security** will produce Awareness campaigns about CoB information to maintain **AFB** staff informed about key points.

15.7.2 Training

Yearly, **IT Security** staff will participate in training activities about Business Continuity, to be updated about last market news and CoB techniques. These activities can include but are not limited to:

- Information Security / Resilience / Business Continuity event attendance.
- Internal training.
- Business continuity / Resilience providers demo / visits.
- Business Continuity / Resilience online Webinars attendance.
- Participate on Forums or Working groups related to COB.

15.8 Testing

Business and technology testing must verify that processes can be recovered in line with the Business's continuity objectives at least **annually**.

The CoB program will be tested following the CoB Testing process to ensure that are consistent with business objectives defined. The tests must ensure:

- That Business Recovery Plan (BRP) and related plans and processes are consistent with the scope and objectives of the CoB.
- Involve all interested parties to verify the results (IT Security, IT and Business units) as needed.
- Produce formalised post-test reports with outcomes, recommendations, and actions to implement improvements.

15.8.1 Retests

Businesses must reattempt failed tests following the CoB Testing process.

15.7 Insurance Cover

Obtaining an insurance policy does not constitute an alternative for the Business Continuity Plan because its objective is not the restoration of the service but only to compensate for the damages caused by the disaster. Various types of insurance exist depending on the IT resource to be covered.

16 COMPLIANCE

16.1 Legal Compliance

AFB will ensure compliance with the highest rigor of all legal, regulatory, or contractual requirements that may be applicable to it based on Organisation's own business activities.

- Be established figures responsible for identifying laws and regulations concerning information security, in order to ensure **AFB**'s compliance. To this end, all national and regional forum means available to the scope of the Organisation, as official gazettes, EU debate, official statements, etc. will be used.
- Regarding legal compliance, special attention should be paid to the regulations established by the new European Data Protection Regulation **GDPR**, replacing the previous Law 15/1999 LOPD from 25 May 2018.
- **GDPR** constitutes a new legal framework on personal data protection and on free circulation and establishes obligations for personal data processing, whose failure can result in very high economic penalties and a negative impact on the **AFB** brand.

Any user processing or accessing to such data must protect the honour, personal and family identity of customers, suppliers and any third party related to **AFB**.

- Workers must only use or reproduce data after obtaining express consent from the owner, while respecting intellectual property rights. Therefore, any reproduction, forwarding, or otherwise representation or redistribution of text, graphics, or other material protected by copyright will be done only with consent from the copyright holder.
- For employees or a temporarily hired provider who use network systems and applications and programs protected by copyright acquired or developed by **AFB**, making copies is strictly prohibited. In any case, it is mandatory to obtain authorisation from the *Data owner* or *CISO*.
- Customer information must be protected from anyone (internal or external) without authorisation to it. This data relates both to information generated during contractual relationship between the client and the entity, as well as the information initially provided by the customer. A Non-Disclosure Agreement (**NDA**) must be signed between the client and **AFB**.
- No **AFB** external staff may have access to any confidential customer data. Only the minimum of people inside company may access customer data and have the right to perform activities for which the company has been hired.

16.2 Regulations and Security Policies Compliance

AFB's different area Managers will ensure adequate review and improvement of the Security Policy, Procedures, and Technical instructions.

Regular independent internal or external reviews will be conducted to verify proper compliance with them and propose corrective action.

16.2.1 Security Audits

Audits and checks will be conducted on a regular basis to verify compliance by the different **AFB** business units with internal security standards.

Audits may be conducted internally or by third parties. If outsourcing audits to a third-party, external consultants must provide specialised knowledge that exceeds internal experience. In the case of subcontracting, guidelines and regulations regarding security for third-party access must be followed.

17 REVIEW AND VALIDITY OF THIS DOCUMENT

This Policy & Standards, its development and application, as well as any other point included in this document, must be reviewed at least once a year by **IT Security** to verify its correct compliance. This review must take into account changes in the current legal framework, audits results and risk analysis carried out since the last review.

On an extraordinary basis when there are material changes that may have an impact on compliance with this Policy & Standards, a review must be carried out to ensure proper compliance.

This Policy & Standards shall apply from the next working day after the date of its publication and shall remain in force until modified or repealed by a later Policy.

17.1 Non-compliance with Policy & Standards

Manifest non-compliance with the guidelines set out in this Policy and all related documents will lead to the application of disciplinary measures that **AFB** deems appropriate, depending on each case.