Overview technical and organisational security measures within Proximus

1. Proximus Security organization

The **Security Governance and Investigation department**, under **Group Corporate Affairs** is entitled with the organization's Security Governance, Security Management and Cyber Security Monitoring and Response responsibilities

Security Governance is responsible for the Information Security Framework of Proximus, which includes the definition and management of the Information Security Policies, as well as of the Security Architecture.

Security Management is responsible to evaluate the alignment of the different company projects with the security policies, to execute information security risk assessments on projects, to execute vulnerability management and pentest management activities and to measure and report compliance to information security policies.

Under **Cyber Security Intelligence & Incident Response** there are two teams:

- Cyber Defense Center - The Cyber Defense Center is the central monitoring team for cyber security incidents on Proximus Group infrastructure and services. With a 24x7 capability using the global Network Operations Center, the Cyber Defense Center aims to detect and contain attacks and intrusions on the shortest possible timeframe.
- Proximus CSIRT - The Proximus CSIRT provides information and assistance to reduce the risks of cyber security incidents as well as responding effectively to such incidents when they occur.   They strive to be an international example for Cyber Security Intelligence and Expertise throughout all areas of Incident Response.   The Proximus CSIRT gathers, filters, analyses and disseminates threat intelligence in order to proactively communicate about upcoming attacks against the Proximus Group.

For each of Proximus core divisions a liaison Security Officer has been appointed to directly coordinate within Security Governance and Investigation, ensuring their division compliance with established Security Framework

2. Proximus Security policy framework

Proximus maintains a Proximus Security Policy Framework which contains comprehensive controls and coverage of current and emerging information security topics that enable the organisation to respond to the rapid pace at which threats, technology and risks evolve. Throughout the established Security Policy Framework, Proximus ensures that information risks associated with its services are kept within acceptable levels, responding to rapidly evolving threats, including sophisticated cyber security attacks and complying with applicable regulations at all times.

Proximus Security Policy Framework is adhering to the best practices of ISF Standard of Good Practice for Information Security providing complete coverage of the topics set out in ISO/IEC 27002:2013, COBIT 5 for Information Security, NIST Cybersecurity Framework, CIS Top 20 Critical Security Controls for Effective Cyber Defence and Payment Card Industry Data Security Standard (PCI DSS), acting as an enabler for continuously improving information security within the organization and helping the organisation to prepare for and manage major incidents that may have a significant impact on Proximus business.

Proximus Security Policy Framework is consistent with the structure and flow of the ISO/IEC 27000 ‘suite’ of standards, and acting as an enabler to multiple ISO 27001 certification programs within the Organization, via the implementation of an Information Security Management Systems (ISMS).

Proximus Security Policy Framework indicatively addresses topics in the areas of :
Human resource, Asset management, Access control, Cryptography, Physical and environmental security, Operations security, Communications security, System development and maintenance, Supplier relationships, Information security incident management, Business continuity management, Compliance.

3. Proximus Security Risk management

The Security Risk Assessment process is a core element in safeguarding security and data privacy at Proximus.

The SRA process guarantees for all projects and systems the implementation of Proximus security controls and an approval by security experts before bringing in service.

The Proximus Risk Assessment Methodology is aligned with the IRAM2 methodology from ISF. IRAM2 is the standard corporate methodology be used across all Proximus wide Information Security Projects and Proximus applied Information Security

Management Systems based on ISO27001. IRAM2 is aligned with the ISF Standard of Good Practice for Information Security.

4. Human resource

The objective of Human Resource security controls are to:

- To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.
- To ensure that employees and contractors are aware of and fulfil their information security responsibilities.
- To protect the organization's interests as part of the process of changing or terminating employment.

5. Asset Management

Proximus asset management and data classification is in place to ensure traceability and auditability.

The objective of Asset Management security controls are to:

- To identify organizational assets and define appropriate protection responsibilities.
- To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.
- To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

6. Access control

Proximus has established methods of restricting access to business applications, systems, computing devices and networks by requiring users to be authorized before being granted access privileges, authenticated using access control mechanisms and subject to a rigorous sign-on process before being provided with access.

Proximus has dedicated Identity and Access Management platforms for its customers, partners and employees to ensure segregation of duties and also a specific infrastructure for privileged access management.

The objective of Access control security controls are to:

- To limit access to information and information processing facilities.

- To ensure authorized user access and to prevent unauthorized access to systems and services.
- To make users accountable for safeguarding their authentication information.

To prevent unauthorized access to systems and applications.

7. Cryptography

Encryption brings an even higher level of security and privacy to our services.

As the data you create moves between your device, Proximus services, and our datacenters, it is protected by security technology like HTTPS and Transport Layer Security.

Proximus encrypts highly confidential and sensitive personal data whenever it is necessary.

Proximus security policies also include the use of pseudonymization (replacing personally identifiable material with artificial identifiers) and encryption (encoding messages so only those authorised can read them).

The objective of cryptographic controls are to ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information**.**

8. Physical and environmental security

The objective of Physical and environmental security controls are to:

- To prevent unauthorized physical access, damage and interference to the organization's

  information and information processing facilities.
- To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.

9. Operations security

The objective of Operations security controls are to:

- To ensure correct and secure operations of information processing facilities.
- To ensure that information and information processing facilities are protected against malware.
- To protect against loss of data.
- To record events and generate evidence.
- To ensure the integrity of operational systems.
- To prevent exploitation of technical vulnerabilities.
- To minimise the impact of audit activities on operational systems.

Specifically, to the exploitation of technical vulnerabilities, Proximus has established a Vulnerability Management process to complete the security cycle involving the projects lifecycle (preventive controls) and the incident response management (detective controls) using a combination of commercially available and purpose-built in-house tools, intensive automated and manual penetration testing, quality assurance processes, software security reviews, and external audits.

Proximus Vulnerability Management process identifies and classifies vulnerabilities, and coordinates remediation and mitigation actions for vulnerabilities which can be caused by
(1) design mistakes,
(2) coding mistakes or malicious code, or
(3) configuration mistakes
and affect elements from
(a) operating systems components or network components
(b) middle components (interpreters, JRE,…) or
(c) daemons, applications, firmwares,…

When vulnerabilities are identified, a corrective path is triggered, involving changes in network, installation of security patches, correction of misconfigurations, correction of applications code or design. This lets Proximus detect and respond to threats to protect products from spam, malware, viruses, and other forms of malicious code.

10. Communications security

The objective of Communications security controls are to:

- To ensure the protection of information in networks and its supporting information processing facilities.
- To maintain the security of information transferred within an organization and with any external entity.

11. System development and maintenance

Proximus design with security in mind. Our security and privacy experts work with development teams, reviewing code and ensuring products utilize strong security protections.

The objective of System development and maintenance controls are to:

- To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.
- To ensure that information security is designed and implemented within the development lifecycle of information systems.
- To ensure the protection of data used for testing.

12. Supplier relationships

The objective of Supplier relationships controls are to:

- To ensure protection of the organization's assets that is accessible by suppliers.
- To maintain an agreed level of information security and service delivery in line with supplier agreements

In detail, Proximus limits access to your business's data to Proximus personnel who need it to do their jobs; for example, when a customer service agent assists you in managing your data.

Strong access controls are enforced by organizational and technical safeguards. And when we work with third parties, like customer support vendors, to provide Proximus services, we have them signed a security schedule document which highlights Proximus security requirements and we audit them randomly to ensure they provide the appropriate level of security and privacy needed to receive access to your business's data.

13. Information security incident management

The objective of Information security incident management controls are to ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

Security Monitoring and Response is one of the core services provided by Proximus Cyber Defense Center and the CSIRT team.

The Security Monitoring and Response Process has been established within Proximus to achieve the following key objectives :

- Provide guidance during decision-making associated with security incidents.
- Provide a process framework for effective 24x7 security monitoring (Level 1) and on-call response service (Level 2 and above) within Proximus, focused on initial detection, analysis and response.
- Provide guidance regarding prioritization and escalation of security incidents.
- Ensuring the Proximus and its customers have the following benefits:
- Improved overall incident resolution through consistent and timely handling of the security incidents monitoring, analysis, identification and escalation.
- Improved service through defined work interfaces with all teams involved in handling incidents.
- Improved and consistent reporting to facilitate continuous improvement of security at Proximus.

Proximus in compliance with international security standards and requirements, has a security logging policy defining all relevant data to be sent to Proximus SIEM platform to perform accurate monitoring of security events.

14. Compliance

The objective of Compliance controls are to:

- To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.
- To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.

* * *