Viewplus Ireland Limited /Ordis UK Ltd
Cyber and Information Security Policy (Incorporating Response Plan)

Table of Contents

1 Introduction

1.1 Policy Objective

This policy is applicable to both Viewplus Ireland Limited and its UK entity Ordis UK Limited.

Viewplus Ireland Limited / Ordis UK Ltd is committed to the preservation of confidentiality, integrity and availability of information to maintain business continuity and minimise the risk of business damage or stakeholder detriment by preventing or limiting the impact of information security incidents. This Policy aims to:

- Maintain effective Information and Cyber Security Risk Management across the business as part of the overall risk management framework of the Company;
- Ensure that cybersecurity roles and responsibilities are clearly defined, documented and communicated to relevant staff;
- Ensure that sensitive information is available to appropriate individuals when required;
- Safeguard the integrity and completeness of information and processing methods;
- Provide the foundation for information security management within the organisation; and
- Enable compliance with key regulatory requirements including GDPR and give due consideration to leading industry standards, frameworks and guidelines.

1.2 Definitions

Cyber-attack: The use of an exploit by an adversary to take advantage of a weakness(es) with the intent of achieving an adverse effect on the IT environment.

Cyber risk: The combination of the probability of an event occurring within the realm of a company's or person's information assets, computer and communication resources and the consequences of that event for a company or person.

Cybersecurity: The measures and controls that ensure the preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium**.**

Cybersecurity risk management: The process used to establish an enterprise-wide framework to manage the likelihood of a cyber-attack and develop strategies to mitigate, respond to, learn from and coordinate its response to the impact of a cyber-attack. The management of a company's cyber risks supports the business processes and is integrated into the company's Risk Management Strategy and Policy (RMSP).

Information assets: refer to data, hardware, software, networks or other elements of a company's IT landscape that support information-related activities. Information Assets are considered by the information owner as an important asset that contributes to the success of the business function(s) that make use of the information. It includes any data or information:

- That is owned by the Company; or
- Resides on information systems or devices of the Company, its employees or contractors; or

- Is generated, collected or distributed by the Company in its course of doing business.

Information Owner is a senior management-level staff member who may authorise or deny access to specific information assets and is accountable for its confidentiality, integrity and availability. The information owner has a firm understanding of the various ways that the information in question is used within their business area.

Information security concerns the company's own information assets and how their confidentiality, integrity and availability are protected.

Information Security Incident is an event that adversely affects or has the potential to affect the confidentiality, integrity or availability of sensitive information. An Information Security incident implies harm or the possibility of harm to sensitive information. Also referred to as an "incident" in the context of this framework.

Personal Data means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Security event: Any observable occurrence in a system and/or network. Events sometimes provide an indication that an incident is occurring.

Security incident: An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Sensitive Information is information assets that would adversely affect the Company, its clients or staff in the event their confidentiality, integrity or availability thereof is compromised. Sensitive information is categorised on a high level, as follows:

- Personal Client Information
- Personal Staff Information
- Special Personal Information
- Intellectual Property
- Business Information.

The Company means Viewplus Ireland Ltd/ Ordis UK Ltd

Full name of legal entity: (**Ireland**) Viewplus Ireland Limited and (**UK)** Ordis UK Ltd Postal address:

Ireland - The View, Marina Village, Malahide, Dublin, K36 CX99, Ireland

UK- Unit D Pendyris St, Cardiff CF11 6BH with the Company Number 17083318

.

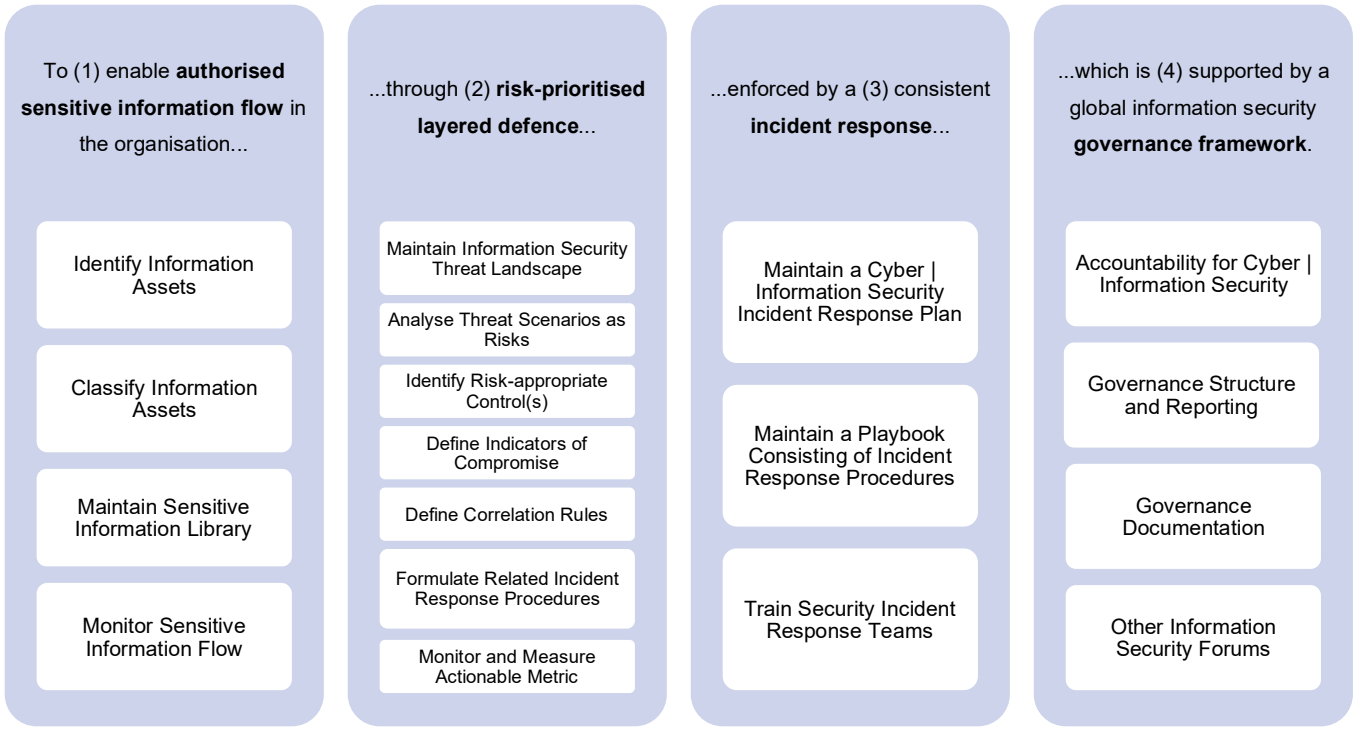
Vulnerability: A weakness in a system, application, or network that is subject to exploitation or misuse.

1.3 Scope and application

The policy covers all business functions, divisions and departments, including outsourced functions of Viewplus Ireland Limited / Ordis UK Ltd . All references made in the document to "Viewplus Ireland Limited ", "the Company" or equally refer to Viewplus Ireland Limited and its UK entity Ordis UK Ltd.

2 Cyber and Information Security Strategy

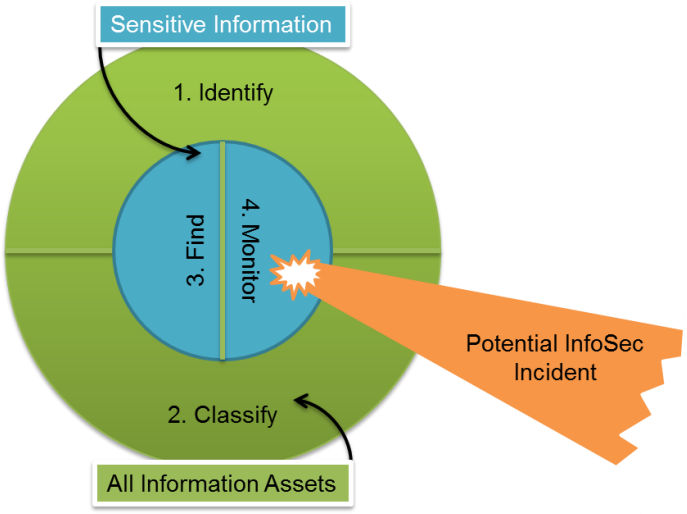
The diagram below sets out Viewplus Ireland Ltd / Ordis Uk Ltd high-level Cyber and Information Security risk strategy through four stated objectives. These objectives are mapped to the enabling principles and the control environment which include the risk and control measures, processes, policies, procedures, plans as well as the governance framework which support the effective implementation of the risk strategy.



The above objectives, enabling principles, and associated risk, control and governance measures are unpacked in sections that follow.

3 Enabling Principles and Control Environment

3.1 Authorised Sensitive Information Flow



<table>
<tr>
<td>1. Identify Information Assets</td>
<td>

Manual sensitive information asset discovery occurs by conducting workshops with senior business management representatives. These workshops are known as “information flow” discovery workshops and are conducted as and when information is required to be updated.
Workshops may include mapping of key business processes, activities, functions, roles and information assets with a view to identify their importance and their interdependencies to Cyber and Information Security risks. The outputs of the workshops are sensitive information flow maps per functional business area.
Sensitive information flow maps are enriched using the “Five Know” principles to identify information security risk during workshops and requirements phase for new projects:

<table>
<tr><th>Know the value of our data</th><th>Know who has access to our data</th><th>Know where our data is</th><th>Know who is protecting our data</th><th>Know how well our data is protected</th></tr>
<tr><td>“The value of our data – to our organisation and customers</td><td>“Who has access both within our organisation</td><td>Locally or with a service provider. Have they provided our data to</td><td>Who is protecting our data and what operational security</td><td>What our security professionals, employees, business</td></tr>
</table>
</td>
</tr>
</table>

	but also the value to those who may wish to compromise it."	and externally."	other third parties? Is it onshore, offshore or in a cloud platform?	processes are in place.	partners and third-party vendors are doing to protect our data.
	• Automated information asset identification is performed through deployment of data discovery tools as required.				
2. **Classify All Information Assets**	Understand the intended business uses of the identified information assets to determine the importance of the following information requirements below. • Confidentiality – ensuring that information is accessible only to those authorised to have access. • Integrity – safeguarding the accuracy and completeness of information and processing methods. • Availability – ensuring that authorised users have access to information and associated assets when required.				
	Several criteria are considered for each category of information asset and articulated in an Information Classification and Protection Policy. Criteria include: • Value of information asset; • Legal and regulatory requirements; • Criticality to the business; and • Level of harm to business if misused.				
3. Maintain Sensitive Information Library	Using the output of manual and automated information asset discovery, an inventory of the sensitive information in the environment is built through determining the location of sensitive information in the IT infrastructure and physical information stores. This is captured in the sensitive information library.				
	A business owner is assigned to each type of sensitive information and is known as the information owner.				

4. Monitor Sensitive Information for Potential Incidents	Sensitive information is proactively monitored for potential incidents in two ways: 1. Automated sensitive information leak-detection techniques deployed in such a manner to detect potential misuse of: • Sensitive information in use (on end-point devices); • Sensitive information at-rest (stored on databases and file servers); and • Sensitive information in-motion (data and email flow across the network perimeter). 2. Scenario-based indicators of compromise (IOC's) based on behavioural exceptions of people and systems that interact with sensitive information. Alerts and exception reports are used as a means for this monitoring technique. The following types of scenarios-based IOC's may be implemented. • Behaviour-based exceptions: ○ For example, a user runs many different reports containing phone numbers in short time-period inconsistent with normal operations. • Access exceptions: ○ For example, a user runs a report that is not authorised within their skillset. • Suspicion of sensitive data abuse: ○ For example, a query is run containing more than 100 phone numbers. • Nature of data: ○ For example, always alert when report contains a bank account number. • Explicit monitoring of specific individuals: ○ For example, alert when any employee who is working while still in their notice-period and accesses sensitive information.
	The Information Security Investigations Forum takes responsibility for monitoring of sensitive information for potential incidents. Potential incidents are registered as cases and investigations are conducted in accordance with the Cyber | Information Security Incident Response Plan.

3.2 Risk-prioritized Layered Defense

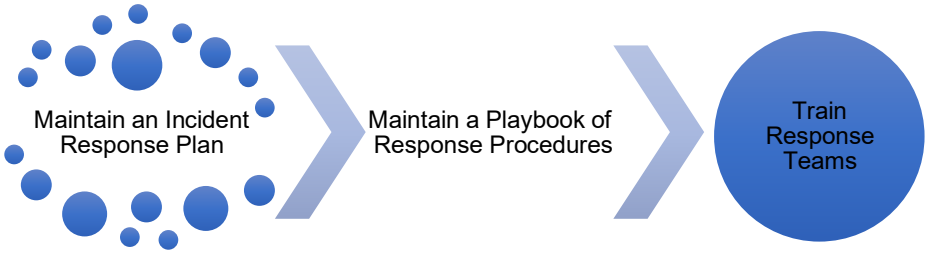
<table>
<tr>
<td>1. Maintain Information Security Threat Landscape</td>
<td>

Threats to the confidentiality, integrity and availability of sensitive information are identified through a scenario-based threat-modelling exercise. Threats are modelled through identifying the following in relation to sensitive data in the environment to construct the Cyber | Information Security Threat Landscape:

<table>
<tr><td>Threat Scenario Description</td><td>Description of scenario that could affect the confidentiality, integrity or availability (CIA) of sensitive information.</td></tr>
<tr><td>Information Asset(s)</td><td>Information assets which may be compromised in the threat scenario.</td></tr>
<tr><td>Threat Actors</td><td>Insider or outsider person(s) who may be involved in the threat scenario.</td></tr>
<tr><td>Attack Vector(s)</td><td>Techniques that may be used to obtain sensitive information maliciously in the scenario.</td></tr>
<tr><td>Threat Driver</td><td>Likely motivation behind the attack.</td></tr>
</table>
</td>
</tr>
<tr>
<td>2. Analyse Threat Scenarios as Risks</td>
<td>Analyse risks related to each threat scenario by assigning an impact and likelihood-rating to the scenario.</td>
</tr>
</table>

3. **Maintain Risk-appropriate Control Baseline Standards**	Plan and implement risk-appropriate controls. The Information Security Control Catalogue may be used as a reference to identify appropriate controls. Key security controls are grouped according to theme, and documented into control baseline standards as they relate to the below information security Capability Areas (refer to Appendix A, for definitions). 
4. Define Indicators of Compromise (IOC's)	It is essential to monitor the environment to determine whether a threat has been realised. To this end, IOC's are identified and documented for each defined threat-scenario.
5. **Formulate Related Incident Response Procedures**	In the event that an IOC is triggered, a consistent and complete response to the potential incident is required. To achieve this, information security incident standard operating procedures are documented for likely threat scenarios. More information is provided in the section on incident response.
6. **Monitor and Measure Actionable Metrics**	Key information security controls are monitored through defined effectiveness metrics to confirm whether they are operating and doing so effectively. The Security Operations Dashboard may be used to maintain key metrics. • IOC's are monitored mainly through exceptions noted in the Security Information & Event Management (SIEM) solution. • The monitoring and measuring process is to (1) measure, (2) analyse trend, (3) follow up on exceptions. • Metrics are measured only if an action can be linked to the result of a measurement.

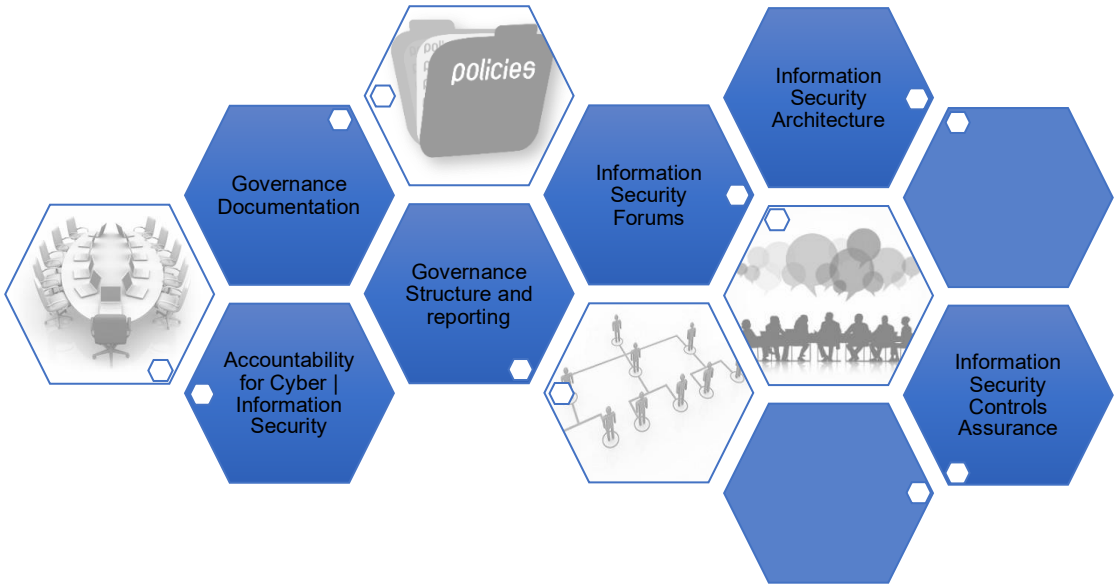
3.3 Consistent Information Security Incident Response



Maintain an Incident Response Plan (CSIRP) Refer to Appendix B	A Cyber and Information Security Incident Response and Recovery Plan is maintained to set out the phases of incident response that are followed for all identified incidents. In short, we refer to it as the Cyber Security Incident Response Plan (CSIRP). The plan consists of the steps below. 1. **Prepare** – ensure that the CSIRP is implemented effectively through adequate awareness and training. 2. **Identify and Validate** – detect the occurrence of an incident and rule out the possibility of it being a false positive. 3. **Contain** – stabilise the environment and secure the area without compromising evidence. 4. **Eradicate** – fix the problem before putting resources back online by addressing root cause. 5. **Recover** – restore systems to original state once root cause has been addressed. 6. **Follow-up & Lessons learnt** – debrief on incident handling process and identify improvements to response plan and information security controls.
Maintain a Playbook of Response Procedures	To facilitate a consistent and complete incident response, information security incident standard operating procedures (response playbooks) are maintained for likely threat scenarios. Each playbook steps through the phases of the CSIRP as it would apply to that specific scenario. Essentially a playbook is a practical implementation of the theory that is defined in the CSIRP.
Train Response Teams (SIRT's)	In the event that an Information Security incident is identified, a Security Incident Response Team (SIRT) is established. The team may consist of one or more representatives from appropriate functions across the Company. Each incident's SIRT is unique and may be made up of members from the following functions or roles (among others): • Information Security

	• Risk Management • Compliance • IT Support or Development • Head of affected business area • Communications • Other appropriate Executive Committee Representation The likely SIRT members for each defined threat scenario are trained on the contents of the CSIRP and playbooks that relate to them to ensure that incident response is optimal.

3.4 Information Security Governance Framework



3.4.1 The Cyber and Information Security Function

Viewplus Ireland Limited / Ordis UK Ltd maintains a Cyber and Information Security Function with a dedicated Head of Cyber and Information Security. This function is supported by a team of Cyber and Information Security specialists of the Company in terms of an outsourcing agreement. The Outsourcing Policy is applicable.

3.4.2 Governance Structures

Accountability for Information Security	The Board of Directors is accountable for the security of information. The responsibility for information security management is delegated to the Executive Committee (Exco) and the IT Cyber and Information Security Forum. This Forum[1] comprises executive and senior management representatives including: • Chief Executive Officer • Chief Information Officer • Chief Operating Officer • Chief Financial Officer • Chief Risk Officer • Head of Compliance • Head of Internal Audit • Heads of IT Support and Development • Members of the Information Security Investigations Forum • Technical Infrastructure Manager / Technical Information Security Architecture Representative • Information Security Manager
Governance Structure and Reporting	The following Committees provides oversight, receive reports and information regarding Cyber and Information Security matters: • The Board: has ultimate responsibility and oversight over Cyber and Information Security risk, the Board is notified of confirmed breaches or incidents requiring escalation as per section 6; • The Board Risk Committee (BRC): the BRC has specific risk management responsibilities and oversight authority. The BRC review and discuss Cybersecurity risk reports received and approves related policies, the BRC is also notified of incidents leading to information breaches; • The Executive Committee (Exco): management committee with the responsibility to ensure that Cybersecurity risks are effectively identified, and mitigated and that appropriate strategies, policies, processes and systems are in place to manage, monitor and report on such risks. Review, challenge and discuss reports. • Risk and Compliance Forum: receives risk management reports including IT and Cybersecurity risks and incident reports. Exco delegates certain tasks to the Forum.

[1] Supported by the Company.

<table>
<tr><td></td><td>

IT and Cyber Security Forum: IT and Cyber Security specialists with the responsibility to focus on Cybersecurity Risks and associated activities.
Operations Forum receives reports as Cybersecurity impacts operations.

</td></tr>
<tr><td>Information Security Forums</td><td>Information Security Investigations Forum – The forum responsible for Data Loss Prevention (DLP) monitoring in each company entity. The forum consists of representatives with appropriate operational knowledge of the business.
Company Information Security Strategy Forum – A forum comprising the information security teams of entities within the Viewplus Ireland Limited / Ordis UK Ltd (“the Company”). The forum aims to facilitate knowledge sharing and strategic alignment (where appropriate).</td></tr>
<tr><td>Information Security Architecture</td><td>Security reference architecture and related requirements are defined. It is the responsibility of solution owners to ensure that security reference architecture is applied. Architecture Review Forums are established to govern this process.</td></tr>
<tr><td>Information Security Controls Assurance</td><td>Activities are undertaken and commissioned by management to gain assurance over the effectiveness and coverage of security controls. This may include:

Monitoring of control effectiveness metrics
Security controls testing
Penetration testing
Capability maturity assessment and benchmarking

</td></tr>
<tr><td>Information Security Governance Documents</td><td>The table below summarise the key governance documents as they relate to the cyber and information security goals.
<table>
<tr><th>Authorised Sensitive Information Flow</th><th>Risk-Prioritised Layered Defence</th><th>Consistent Incident Response</th><th>Global Information Security Governance</th></tr>
<tr><td>Sensitive Information Flow Maps</td><td>Cyber / Information Security Threat Landscape</td><td>Cyber / Information Security Incident Response Plan (CSIRP)</td><td>Terms of Reference of Committees</td></tr>
<tr><td>Information Classification Standard and Handling Guidelines</td><td>Control Baseline Standards per Capability Area</td><td>Information Security Incident Standard Operating Procedures (Playbooks)</td><td>Documented Target Operating Model for Information Security</td></tr>
</table>
</td></tr>
</table>

	Sensitive Information (DLP Rule) Library	IOC and Correlation Rule Library	Security Operations Dashboard	

4 Cyber and Information Security Risk Management

Risk Management and assurance activities relating to Cyber and Information Security risks are performed in line with the identified Cyber and Information Security goals and the RMSP.

4.1 Risk Appetite Alignment

4.1.1 The risk appetite is set out in the Risk Appetite Framework (RAF) as approved by the Board.

4.1.2 Risks associated with Systems include Technology Driven Business Enablement, Critical System Availability and Cyber and Information Security. Overall, Viewplus Ireland Limited / Ordis UK Ltd maintains a low-risk appetite for Systems risk, however within this risk type, the risk appetite for Cyber and Information Security is medium given the high inherent risks associated with the external environment, the risks associated with strategies around systems transformation and the fast-changing landscape of cyber-attacks. While a low residual risk is preferable for the Cyber and Information Security risk type, it is aspirational, and the costs and resources required for risk management within a low appetite are some of the factors considered. Our appetite for risks associated with customer data privacy and treating customers fairly is low as stated in the Processes Risk category of the RAF.

4.1.3 Key Risk Indicators are documented and maintained in the RAF and not repeated here.

4.2 Risk Definition and Sources

The high-level risk definition is tabled below which is an excerpt from the Risk Classification table as documented in the RMSP showing examples of the associated risk causes or drivers.

Risk Types	Definition	Possible Causes / Drivers
Cyber & Information Security	Risks associated with the confidentiality, integrity and availability of sensitive information.	- Inadequate Cyber Governance and monitoring - Inadequate Physical security - Data theft/malicious manipulation - Unintentional data loss - Cyber-attacks and events - Improper access to data - Inadequate Training and awareness; Poor Culture - Applications developed with security vulnerabilities - Failure to protect, detect or respond to customer or employee privacy and personal information, intellectual property or other sensitive or confidential data compromise. - Process Failures (Vulnerabilities, Patch, Supplier, Incident Response Management) - External party information sharing inadequately managed

4.3 Risk Identification

4.3.1 Risks and the associated mitigating controls are identified during regular scheduled risk and control assessment workshops.

4.3.2 These workshops are held between Risk Management, each Risk Owner and relative members of the business, at least annually.

4.3.3 Blank page reviews are conducted and emerging risks considered.

4.3.4 All risk types are also identified during daily activities by Risk Owners and management.

4.3.5 Controls are identified and rated in accordance with the process described in the RMSP.

4.3.6 Where new products, processes and systems are planned or introduced risk identification and assessments shall also be undertaken. Monitoring takes place as described in the RMSP.

4.3.7 Monitoring of KRIs is utilised to assess the accuracy of risk ratings by comparing observed KRIs with the residual risk ratings. These are set out in the RAF.

4.4 Risk Measurement

4.4.1 Operational risk identification and assessment is conducted in line with the processes and procedures described in the RMSP.

4.4.2 Risk rating takes place based on the Viewplus Ireland Limited / Ordis UK Ltd Risk Rating Matrix.

4.4.3 Details regarding the functionality of the Risk Management system are set out in the RMSP.

4.5 Resourcing, Training and Awareness

4.5.1 Resourcing

Viewplus Ireland Limited / Ordis UK Ltd employs and contract with appropriately skilled resources to ensure that IT operational and risk management processes are adequately supported and that Cyber and Information Security risks are managed.

4.5.2 Training

4.5.2.1 IT resources receive training on a regular basis on relevant topics.

4.5.2.2 Training is provided regarding the content of this Policy.

4.5.2.3 Several Training activities and programmes are provided by the IT function to all employees. Training is of ongoing nature to ensure awareness of the risks and how to avoid pitfalls around cybersecurity and related IT risks.

4.5.2.4 The Online Training includes topics such as:

- Passwords
- Phishing

- Information Protection
- Data in Motion
- Virtual meeting hygiene
- Data Privacy.

4.6 Combined Assurance

4.6.1 The Combined Assurance Model

The Combined Assurance Model is applied to all IT Risk mitigating strategies, including Cyber and Information Security Risk as follows:

- First line of defence: Assurance is provided by IT management team under the leadership of the CIO through the IT monitoring and reporting structures and process governance outputs described earlier in the IT Governance Framework. IT Leadership is also responsible for implementing corrective actions to address process and control deficiencies.
- Second line of defence: IT Risk Management facilitates and monitors the implementation of effective IT risk management practices in line with the RMSP to ensure that key business risks relating to IT are appropriately managed in line with the RAF. The Head of Compliance ensures that any regulatory requirements and / or changes are communicated to all the stakeholders with a view to update policies, procedures, processes and systems. The Head of Compliance also facilitates any reporting needed to the authorities.
- Third line of defence: Internal Audit provides assurance on the effectiveness of internal controls, including independent reviews of the control environment. Auditors with sufficient knowledge, skills and expertise provide independent assurance of Viewplus Ireland Limited / Ordis UK Ltd governance, systems and processes for its Cyber and Information Security risks to the Board. The frequency and scope of these audits aim to be commensurate with the relevant risks.

4.6.2 The Combined Assurance Forum

Viewplus Ireland Limited / Ordis UK Ltd has established a Combined Assurance Forum (CAF). The objectives, composition, roles and responsibilities are documented in the Terms of Reference of the CAF. The CAF supports the combined assurance model across the business, assists to accomplish the philosophy behind it and serves to maintain an effective control environment. The CAF also provides a platform for control functions and assurance providers to discuss relevant themes including Cyber and Information Security Risks.

5 Monitoring and Reporting

Cyber and Information Security monitoring, including tests, risks and controls self-assessment and reporting are ongoing.

5.1 Information security testing and monitoring

5.1.1 Viewplus Ireland Limited / Ordis UK Ltd conducts or arranges information security testing to validate the robustness and effectiveness of our information security measures considering threats and vulnerabilities identified through threat monitoring and the risk assessment process.

5.1.2 Testing is carried out in a safe and secure manner and by independent and suitably qualified and skilled testers.

5.1.3 These tests are conducted on a regular basis and the frequency, testing method (such as penetration testing, including threat led penetration testing) and scope is commensurate with the level of risk identified. Testing of critical systems and vulnerability scans are performed annually.

5.1.4 Tests of security measures are conducted in the event of changes to infrastructure, processes or procedures and if changes are made because of major operational or security incidents or due to the release of new or significantly changed critical applications. Results of tests are evaluated and if required, security measures are updated accordingly.

5.1.5 Certain monitoring activities are designed to test awareness of and compliance with this Policy.

5.1.6 Monitoring activities are also described in section 3 of this Policy.

5.2 Reporting

5.2.1 Reports are provided to the relevant governance structures as indicated in section 3.4 of this policy.

5.2.2 Reports include information such as:

- Updates and progress information regarding projects and initiatives (Cyber and Information Security Function);
- Top risks, risk profile and mitigating tasks (Risk Management Function);
- Results from tests, reviews or assessments such as penetration tests, third party reviews or Internal Audit reviews (Reviewer or Cyber and Information Security Function);
- Incident reporting (Cyber and Information Security Function);
- Key Risk Indicator monitoring outcomes (Risk Management Function).

6 Escalation

- Individuals responsible for the respective business areas, committees and forums and Risk Owners must inform the Head of Information Cyber and Information Security, the CIO, Risk Management, Internal Audit, Compliance and Actuarial Control Functions of any facts relevant for the performance of their duties which may impact the effectiveness of the IT Governance Framework and the risk profile.
- In the event that Viewplus Ireland Limited / Ordis UK Ltd becomes aware of a cybersecurity incident that could have a significant and adverse effect on the company's ability to provide adequate services to its customers, its reputation or financial condition, the Board and the Central Bank of Ireland (CBI) shall be notified accordingly as soon as possible.

- Risk outside appetite and KRI breaches are escalated to the Board and CBI as set out in the RAF.
- Any material matters relating to Cyber and Information Security that are not specifically dealt with in this Policy or present an exception to a policy stipulation must be escalated to the CIO for guidance, instruction, or further escalation to the governance structures.

7 Roles and Responsibilities

7.1 Policy Owner - Chief Information Officer

7.1.1 The policy owner is responsible for ensuring the policy is maintained and that it addresses relevant legal, regulatory and other key documents.

7.1.2 The policy owner manages the process for updating the policy in accordance with the Review timing outlined in this policy.

7.2 The Cyber and Information Security Function

The roles and responsibilities of the function include:

7.2.1 Supporting the Board and the Board Risk Committee in maintaining this Policy and the effective communication, training and deployment.

7.2.2 Reporting on a regular basis to the respective governance structures and on an ad hoc basis, as may be required, on the status of cyber and information security.

7.2.3 Monitoring, reviewing, updating and implementing information security measures.

7.2.4 Ensure that cyber and information security requirements are adhered to when using outsourcing arrangements and service providers.

7.2.5 Providing for training and awareness to all employees and service providers relating to cyber and information security risks and this policy.

7.2.6 Coordinating operational and / or security incident management and reporting in line with this Policy and the Operational Risk Policy.

7.2.7 Ensure that escalation of material matters take place as set out in section 6 of this Policy.

7.3 All Employees and Service Providers

Due to the nature of Cyber and Information Security risks, all employees at Viewplus Ireland Limited / Ordis UK Ltd are required to:

7.3.1 Participate in the training and awareness activities offered which are designed to ensure understanding of the risks and the stipulations of this Policy;

7.3.2 Be vigilant in identifying risks and reporting same to the Cyber and Information security function;

7.3.3 Comply with the stipulations of this Policy.

The Cyber and Information Security Policy requirements are included in communication to and formal contracts with service providers.

8 Approval and Review

- This policy is approved by the Board Risk Committee (BRC).
- The Policy will be reviewed at least annually by the CIO or a person appointed by the CIO to ensure its ongoing appropriateness, its continued alignment with all other policies, risk appetite and business strategies and presented to the BRC for approval.
- Where there are non-material changes to this policy, such as formatting, title changes, and simple grammatical errors, these changes can be approved by the Policy Owner who must inform the BRC as part of the standard reporting.
- Any questions on the content of this policy should be directed to CIO.

9 Linked Policies and related documents

9.1 Company Policies

Relevant policies include:

- IT Governance Framework
- Company Cyber Security Framework
- Data Management Policy
- Information Classification and Protection Policy
- Risk Management Strategy and Policy
- Risk Appetite Framework
- Business Continuity (BCP) and IT Disaster Recovery Plans (IT DRP)

9.2 Regulatory Context

- Cross Industry Guidance in Respect of Information Technology and Cybersecurity Risks, 2016
- Guidelines on Information and Communication Technology Security and governance EIOPA-BoS-20/600
- Data Protection Act 2018 (as amended)
- General Data Protection Regulations (EU) 2016/679.

9.3 Standards / Guidelines

- ISO/IEC 27001:2013/2022 – Information technology – Security techniques – ISMS
- ISO/IEC 27002:2013 – Information security techniques – Code of practice
- ISO/IEC 27005 – Information security risk management
- The Centre for Internet Security (CIS) Critical Security Controls for Effective Cyber Defence - Version 7.1
- CIS Top 20 Security Controls
- ISACA's Control Objectives for Information and Related Technology (CobIT) framework.
- Payment Card Industry Data Security Standard (PCI DSS)
- National Institute of Standards and Technology (NIST).

10 Document Control

Version	Policy Reviewer(s)		Approved		Review date
V.1	John Dabill / Sandeep Kannirasan		YES		13th August 2026

11 Appendix A: Cyber and Info Sec Capability Areas Definitions

Capability Area	Defined as dealing with threats related to....
Application Security	...coding and configuration vulnerabilities on centralised enterprise applications which present or process sensitive information and is accessible by a set of users either through web or non-web interfaces.
Cloud Security	...platforms, software or infrastructure which store or process sensitive information and are provided as a service by cloud providers as opposed to being hosted in data centres owned by the Company. Business intelligence platform and underlying database may be hosted in Microsoft Azure®.
Cryptography	...encryption standards, platforms and processes utilised across various infrastructure and system implementations to encode data at rest and in motion. Process for secure storage of public key encryption certificates.
Cyber Incident Response	...inability to identify, manage, record and analyse security threats or incidents in real-time. E.g. - The Active Directory (AD) Self Service Portal which is exposed to the outside is compromised but there are no formal procedures to respond to the incident.
Cyber Security Governance	...inadequate cyber security governance is performed, resulting in priority being placed on the incorrect areas and insufficient controls implemented. For example: Process to decommission unused hosts in the environment is given priority above implementing a proactive patching strategy.
Data Security	...sensitive data at rest and stored in mass data repositories which may be directly accessed by unauthorised individuals. Example: Excel sheet with client information is found on a file server. A decision must be made to encrypt, delete, move, tokenise or limit access to the data.
Email Security	...email sent or received through the Company's email system which may compromise the confidentiality of sensitive information. Example: An unusual number of phishing emails may be successfully delivered to staff inboxes by an attacker.
Endpoint Security	...the ability of attackers to use servers, laptops and PC's as footholds in the organisation or egress points for exfiltration of sensitive information. Example: A laptop may be infected with malware which gives an attacker remote access to execute arbitrary commands on the company's network.

Capability Area	Defined as dealing with threats related to....
Human Security	...the ability of an attacker to circumvent key security controls though the use of various social engineering techniques on staff or contractors with access to sensitive information. A harshly worded email from an attacker posing as an IT executive to an advisor which states that they should click on a link to confirm their active directory login credentials.
Identity and Access Management	...the lifecycle of user accounts on sensitive systems which are allocated to staff or contractors and the privileges which are granted to those profiles. Example: Transactions may be detected on a resigned user's account after their last working day.
Insider Breach Monitoring	...monitoring of probable egress points of sensitive information for malicious and accidental data breach by internal staff, contractors and other authorised system users.
Mobile End Point Security	...the use of mobile devices (such as smart phones and tablets) to access, store or share sensitive information.
Network Security	...our network perimeter as well as the internal network which may be exploited by attackers who make use of network based attack vectors.
Physical Security	...physical locations (including locations other than the head office buildings and data centres) that house operational staff, equipment and other physical artefacts which acquire, access, process, use, store, share or dispose of information assets. It may be possible for an attacker posing as a visitor to enter the call centre without being positively identified.
Privileged Access Management	...staff or contractors with wide access to sensitive systems and thereby have the ability to compromise the confidentiality, integrity or availability of sensitive information on a large scale. For Example: A disgruntled actuarial contractor with privileged access to the data warehouse may be able to delete all databases.
Third-Party Security	...sharing sensitive information with service providers – either routinely or on an ad hoc basis.
Security Event Management	...processing, storage and representation of security event logs to identify and analyse security incidents and control effectiveness. Firewall and server time settings may not be synchronised, resulting in an inability to correlate perimeter network events with activity on the server.

Capability Area	Defined as dealing with threats related to....
Vulnerability Management	...known security flaws which exist on critical infrastructure, operating systems and applications and may be exploited by attackers. ...failures to proactively patch or configure hardware and software platforms in line with leading practice guidelines for optimal security. A remote code execution vulnerability may exist on Adobe flash player which is installed on a PC and is then exploited by ransomware to encrypt all of a user's documents.

12 Appendix B - Cyber Security Incident Response and Recovery Plan

12.1 Introduction

The Cyber Security Incident Response Plan (CSIRP or "Plan") is designed to ensure that Viewplus Ireland Limited / Ordis UK Ltd has the ability to effectively respond to and manage cybersecurity incidents which may compromise the confidentiality, integrity or availability of its information systems, data or network resources. It creates objectives for actionable procedures that can be measured, evaluated, scaled, and revised as necessary.

A Cyber Security Incident is an event that adversely affects or has the potential to affect the confidentiality, integrity or availability of sensitive information. It implies harm or the possibility of harm to sensitive information and is also referred to as an "incident" in the context of this document.

The Plan sets out the various pertinent activities which should be carried out in each of the response phases contained in the diagram below.

12.1.1 Definitions

Data subject	Means the person to whom personal information relates
Honeypot	A mechanism set to detect, deflect or counteract attempts at unauthorised use of information systems.
IT DRP	Information Technology Disaster Recovery Plan of the Company
Personal Information	Means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to— (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person; (b) information relating to the education or the medical, financial, criminal or employment history of the person; (c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person; (d) the biometric information of the person; (e) the personal opinions, views or preferences of the person;

	(f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; (g) the views or opinions of another individual about the person; and (h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.
SIEM	Security information and event management system
SOC	Security Operations Centre whose primary responsibility is to monitor for and alert the Company in the event of the occurrence of cybersecurity incidents.
Tuning	The act of adjusting the rules in an incident detection or equivalent system which was used to identify a false positive incident.

12.2 Incident Response Phases

12.2.1 Preparation

The goal of the preparation phase is to ensure that staff are appropriately trained and are equipped with adequate procedures and tools for detecting and responding to an incident.

12.2.1.1 Proactive Incident Detection Capability

To effectively detect and respond to incidents, the appropriate data needs to be at the disposal of the response team. The following is done to ensure that this is the case:

- Appropriate security and other system events from relevant systems are aggregated into a central repository (also referred to as the security information and event management system, or SIEM).
- The aggregated SIEM logs are correlated to construct automated indicators of compromise (IOC's), which indicate potential threat activity in the environment. IOC's are analysed by the security operations centre (SOC) as potential incidents.

Due to the ever-evolving nature of the cyber threat landscape, the log sources and IOC's above are dynamic and continuously adapting.

12.2.1.2 Reactive Incident Reporting Capability

Mechanisms for reporting incidents which were potentially not proactively detected are made available to both staff and external parties.

12.2.1.3 Cyber Security Incident Response Team

A cybersecurity incident response team (CSIRT, or "response team") is established. The CSIRT identifies, responds to and manages incidents. The CSIRT comprises 3 groups, namely Detection and Response, Coordination and Executive.

At least one member from one or more of these groups are required to form part of an incident's response team, dependent on the priority, validity and impact rating of the incident. The high-level membership, roles and responsibilities of each of the groups are detailed in the table below.

At least one member from each of the above groups must be available at all times to promptly respond in the event that an incident is detected or reported.

Group	Members[2]	Responsibilities
Detection and Response Group	• Security Operations Centre (SOC) • Cyber Security Specialist(s) • Information Security Investigations Forum • IT Support Specialist(s) • IT Development Specialist(s)	• Notifies other members of the response team of a potential incident. • Determines extent of damage to information systems, network resources and/or data. • Recommends course of action. • Carries out containment, eradication, and recovery processes.
Coordination Group	• Incident Handler • Head of Information Security • Head of IT Infrastructure • Relevant IT Infrastructure Manager(s)	• Accountable for the incident response process. • Informs affected operational areas management, users and third-party organizations.
Executive Group	• Chief Operations Officer (COO) • Chief Risk Officer (CRO) • Chief Executive Officer (CEO) • Chief Information Officer (CIO) • Head of Compliance • Relevant General Managers and/or Department Heads	• Invokes Business Continuity or IT Disaster Recovery Plans if required. • Makes financial and staffing decisions. • Communicates with operational management. • Investigations and decisions regarding customer and regulatory communications

12.2.1.4 Business Continuity and IT Disaster Recovery Plan Integration

Provision is made in the Company's Business Continuity (BCP) and IT Disaster Recovery Plans (IT DRP) for cybersecurity incidents which overlap with the mandate of those documents. Relevant sections include, but is not limited to:

- Communication with clients, staff, service providers and regulators in the BCP; and
- Redundancy and backups of critical infrastructure in the IT DRP.

12.2.2 Identification

The Identification phase is focused on determining whether or not an incident has occurred and subsequently determining the type and severity of the incident to ensure the appropriate response.

[2] Teams supported by the Company.

12.2.2.1 Detect the Incident

Primarily, it is the responsibility of the SOC to detect potential incidents through the use of IOC's which are configured in the SIEM. Incidents may also be reported through the mechanisms made available to staff or external parties.

12.2.2.2 Assign an Incident Handler

Once an incident is detected, a CSIRT member or delegate is assigned to coordinate the response to the incident from detection through all response phases to closure. This person is the incident handler.

12.2.2.3 Capture the Incident

The incident handler is responsible for ensuring that the incident is captured on the designated incident tracking system as an open incident. The facts of the incident are captured on the tracking system, including anything that is known about the incident, when and how it was first detected, unusual log file entries or notification alerts as well as other anecdotal reported anomalies.

12.2.2.4 Potential Incident Severity Rating

The priority of an incident is determined using the severity rating criteria set out in the table below as a guideline. The severity rating may be adjusted throughout the lifecycle of the incident as more information comes to light or at the discretion of the incident handler.

Severity	**Short Description**	**Criteria for Potential Data Leak**	**Criteria for Potential IOC**
1	Major Event	• More than *50 records* of *personally identifiable* or other client or staff personal information records. or • *Intellectual property* of the Company that *could cause major harm* to the business if misused.	• Any allowed indicator of compromise on an asset that is highly sensitive, based on the confidentiality, integrity or availability requirements of the data that it processes or stores.
2	Moderate Event	• Between *4 and 50 records* of *personally identifiable* or other client or staff personal information records. or • *Intellectual property* of the Company that is *unlikely to cause harm* to the business if misused.	• Any allowed indicator of compromise on an asset that is moderately sensitive, based on the confidentiality, integrity or availability requirements of the data that it processes or stores. or • Any blocked indicator of compromise on an asset that is

Severity	Short Description	Criteria for Potential Data Leak	Criteria for Potential IOC
			highly sensitive, based on the confidentiality, integrity or availability requirements of the data that it processes or stores. or • Any persistently blocked indicator of compromise on any host.
3	Minor Event	• *Less than 4 records* of *personally identifiable* or other client or staff personal information records. or • *Intellectual property* of the Company that will *under no circumstances cause harm* to the business if misused.	• Any singularly blocked indicator of compromise on any host.

12.2.2.5 Incident Validation

The incident handler examines the facts of the incident and collaborates with other CSIRT team members to determine if indeed a security incident has occurred. Using the information at hand, the incident handler classifies the incident as one of the following:

- *False-positive* – the event incorrectly indicated the occurrence of an incident.
- *False alarm* – the event correctly indicated the occurrence of an incident, but there was no impact on the Company.
- *True positive* – the event correctly indicated the occurrence of an incident and there was an impact on the Company.

False-positive incidents usually result in the need to adjust (tune) the correlation rules in the SIEM or equivalent system that was used to identify the incident to prevent future false positives.

12.2.2.6 True Positive Impact Rating

The impact of a true positive incident is determined through the use of the risk rating matrix contained in the Risk Management Strategy and Policy (RMSP). In accordance with the risk appetite of the Company that is defined in the RMSP, incidents with an impact rating of "Insignificant (1)" are regarded as low impact, while incidents with an impact rating of "Minor (2)" and above exceed appetite and are regarded as high impact for purposes of this plan.

Consequence / Impact					
Description	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Severe (5)

The impact of an incident may be financial, reputational or business disruptive in nature. Refer to the impact rating scale in the RMSP appendices for more detail on the types of impacts that are considered insignificant (1), or minor or more (2 – 5). The incident handler assigns an impact rating to a true positive incident using this scale and their professional judgement as a guide.

12.2.2.7 Incident Notification to CSIRT Groups

The incident handler involves appropriate members of the CSIRT groups at two stages in the response process:

- When potential incident priority has been established; and
- When a true positive incident's impact rating has been assigned.

The table below indicates which groups should be involved based on the priority and impact rating of the incident.

Potential Incident Severity	**Impact Rating**	**Involvement by Response Group Criteria**
Minor Event (Severity 3)	Low	• Detection and Response
Moderate Event (Severity 2)	Low	• Detection and Response
Major Event (Severity 1)	Low	• Detection and Response • Coordination (if required)
	High	• Detection and Response • Coordination • Executive

12.2.2.8 Cyber incidents involving a breach of personal data

Where there are reasonable grounds to believe that personal information has been accessed or acquired by any unauthorised person, the CSIRT Executive Groups must ensure that notification goes to the CBI, any other supervisory authority and data subjects where relevant, unless the identity of the data subject cannot be established. Refer to section 6. The Compliance Function is consulted in the process to ensure that notifications take place as required by legislation, regulation and company policies.

12.2.3 Containment

The containment phase is focused on limiting the impact and magnitude of an incident on the Company. The table below lists the containment activities and indicates under which circumstances each activity is required to be applied.

No	Containment Activity	Low Impact	High Impact
1	*Isolate the host or system – Isolate the compromised host from the network* to prevent the impact the affected host might have on other hosts in the environment.	At the discretion of the CSIRT	Required
2	*Containment Plan* – The CSIRT Detection and Response Group assesses the damage to impacted systems, data and/or network resources. The group then creates a brief plan of action and time estimate to rebuild or repair the impacted information systems, data, and/or network resources, considering the containment activities required by this plan.	Not Required	Required
3	*CSIRT Stand-up* – For all high impact true positive incidents, CSIRT members gather as soon as a true positive has been declared by the incident handler. They are briefed by the incident handler to the progress made against the containment plan.	Not required	At least daily
4	*Forensic Investigators* – One of the specialist forensic service providers (or as advised by the Corporate Cyber Security Insurance Provider) is involved at the earliest point in the investigation if the CSIRT forms the opinion that the outcome of the incident may result in legal action.	Required	Required
5	*Physical Evidence Collection* – The source of the attack is physically located. Care is taken in removing the device from the network and appropriately sealing the device to assist in ensuring chain-of-custody.	Not required	Required
6	*Redundancy and Backups* – In the event that a critical system or data availability-affecting incident occurs, the IT DRP is referred to for redundancy and backup recovery activities.	At the discretion of the CSIRT	At the discretion of the CSIRT
7	*Affected System Backups* – Data backups (full or incremental) of affected systems are performed as appropriate.	At the discretion of the CSIRT	Binary (forensic) backup required
8	*Honeypots* – Carefully consider whether attackers should be diverted to misleading or false systems or information in order to gather more data on the attackers and/or to assist law enforcement agencies. Honeypot devices, honey-accounts and honey-tokens should be considered.	At the discretion of the CSIRT	At the discretion of the CSIRT

No	Containment Activity	Low Impact	High Impact
9	*Maintain a Low Profile* – All precautions are taken to avoid alerting the agent or source of the attack to the fact that the incident is being responded to.	At the discretion of the CSIRT	At the discretion of the CSIRT
10	*Passwords* – Passwords of any system accounts which may have been compromised are changed.	Required	Required
11	*Operational Internal Notification* – The incident handler and CSIRT Coordination Group notifies all appropriate organisations and individuals about the likely operational impacts of the security incident, including but not limited to: • System owners and administrators • Operational management • Third-party service providers • Staff • Clients	Required	Required
12	*Non-operational External Notification* – The CSIRT Executive Group decides on appropriate communication with external parties in consultation with the Compliance department and in line with the provisions set out in the BCP. External parties include, but are not limited to: • Clients • Regulators • The media • Third-party service providers *Note: Notification of external parties occurs as early on in the incident response process as possible. However, it occurs only in the event that the CSIRT Executive Group is comfortable that it has adequate information at hand regarding the validity and impact of the incident. Alternatively, external notification is handled in the Recovery phase of incident response.*	Not required	As appropriate

12.2.4 Eradication

The goal of the eradication phase is to eliminate all adverse impacts caused by a security incident and mitigate the vulnerability(s) that led to the incident to avoid reoccurrence. The table below lists the eradication activities and indicates under which circumstances each activity is required to be applied.

No	Eradication Activity	Low Impact	High Impact
1	*Root Cause Analysis* – The CSIRT Detection and Response Group examines logs, audit records and other appropriate sources (e.g. camera footage) to determine the root cause of the incident. Root cause analysis techniques such as "five whys" are employed.	Required	Required
2	*Perform Vulnerability Analysis* – The CSIRT Detection and Response Group assesses systems impacted by the incident for vulnerabilities.	Required	Required
3	*Improve Countermeasures* – The CSIRT Detection and Response Group takes ownership of the mitigation actions required to address the identified vulnerabilit(ies) that led to the incident.	Required	Required
4	*Rebuild or Repair* – As necessary, the CSIRT Coordination Group determines whether systems impacted by an incident should be rebuilt or repaired. Criteria used to make this decision includes: • type of access and privileges gained by an attacker; • complexity of the attack vectors; • length of the incident; and • time and effort required to rebuild or repair the information systems. All configuration changes, files, applications or malicious code is completely removed from the system(s). All repairs are documented as per the Infrastructure Change Management process. The data and configuration backup provisions set out in the IT DR plan are relied upon.	Required	Required
5	*Most Recent Trusted Backup* – If a decision is made to rebuild a system, the incident handler locates and acquires backup(s) which are known not to be compromised.	As appropriate	As appropriate
6	*Continuous IOC Improvement* – The CSIRT Detection and Response Group determines whether improvements or additions should be made to IOC's in order to better detect future occurrences of the threat(s) that caused the incident.	Required	Required

12.2.5 Recovery

The goal of the recovery phase is to return all data and/or services impacted by an incident to full operational status. The table below lists the recovery activities and indicates under which circumstances each activity is required to be applied.

No	Recovery Activity	Low Impact	High Impact
1	*Validate Information Systems* – The relevant system owner(s) verify that their systems which were rebuilt or repaired during the Eradication response phase are functioning as expected.	As appropriate	As appropriate
2	*Decide When to Restore Operations* – In the event that data or services have been made unavailable to staff, clients or business partners because of the incident, the CSIRT Coordination Group determines when the data or services should be made available again.	Required	Required
3	*Internal Notification of Recovery* – The CSIRT Coordination Group notifies appropriate internal parties when impacted data and/or services are fully available and functional: • System owners and administrators • Operational management • Third-party service providers • Staff	Required	Required
4	*External Notification of Recovery* – When impacted data and/or services are fully available and functional, the CSIRT Executive Group determines an appropriate communication with external parties in consultation with the Compliance department and in line with the provisions set out in the BCP. External parties include, but are not limited to: • Clients • Regulators • The media • Third-party service providers	Not required	As appropriate
5	*Formal Data Breach Reporting* – In the event that an incident resulted in suspected or confirmed loss, theft or unauthorised access of sensitive information, a meeting is organised by the CSIRT Coordination team that includes the CSIRT Executive Group and appropriate EXCO representation. The objective of the meeting is to decide on the method, content and timeliness of formal breach reporting to regulators, clients, media and other external parties.	Not required	As appropriate

12.2.6 Follow-up

The focus of the follow-up phase is to identify lessons that will enable the CSIRP to more effectively respond to and manage the next security incident.

No	Follow-up Activity	Low Impact	High Impact
1	*Conduct a Lessons-Learned Meeting* – Using the Follow-up Questionnaire in Annex B as a guide, the incident handler conducts a lessons-learned meeting. All members of the CSIRP attend the meeting.	Not required (Analysed in SOC Meeting)	Required
2	*Follow-up Report* – The incident handler produces a follow-up report that describes the incident, lessons learned and recommendations for better responding to and managing future incidents. The report is distributed to the Cyber and Information Security Steering Committee.	Not required (Analysed in SOC Meeting)	Required
3	*Implement Approved Recommendations* – Recommendations approved by management are communicated to the appropriate task owners by the incident handler and tracked until implementation.	Required	Required
4	*Incident Closure* – Once the activities in the follow-up phase have been completed, the incident may be marked as closed on the incident tracking system.	Required	Required

12.2.6.1 Follow-up Questionnaire

The list below contains the questions which should be used to guide the follow-up meeting agenda.

- Briefly describe the security incident and what actions were taken.
- How much time was spent responding to the incident?
- What were the costs (direct and indirect) of the incident?
- What did the CSIRT do well in responding to and managing the incident?
- What difficulties were encountered in responding to and managing the incident?
- Was there sufficient preparation by the Company for the incident?
- What preparation was not done that should have been?
- Did the detection of the incident occur promptly? If not, why not?
- What additional tools could have helped to better respond to and manage the security incident?
- Was the incident quickly and sufficiently contained? If not, what additional tools or processes could have helped to contain the incident?
- Was communication among CSIRT members adequate? If not, what could be improved?
- Was communication with management and employees adequate? If not, what could be improved?
- Was communication with external parties adequate? If not, what could be improved?
- Was communication with clients adequate? If not, what could be improved?

- Were remediation procedures adequate to prevent future occurrences?
- Additional information that the CSIRP deems relevant.

12.3 Testing IRP Readiness

The readiness of the Company to successfully apply the CSIRP is tested as detailed in the table below. Response activities which relate or overlap with those in the Business Continuity Plan and IT DR Plan are tested as part of this processes respectively.

Readiness Test	Frequency
"Tabletop" Simulation – This test is facilitated by the Cyber Security Manager and enables the CSIRT to use theoretical scenarios to gain comfort on the readiness of the people, process and technology preparation that was done from a Cyber Security Incident Response planning point of view.	Annual

12.4 The Top 10 "What Not To Do's" In An Incident"

1. **Don't Run Antivirus (AVs):** AVs often change file systems, deleting malware and destroying the metadata crucial for an investigation. Moreover, they often retain little or no logs about what they found, where it was, and when it was put there. If you know there has been a major security incident, be aware that running one or multiple AV products is one of the most destructive actions you can do.
2. **Patching Systems / Fixing Bugs:** Patching systems is recommended, refer to recent news items if you need proof. However, when you find something un-patched on your internet facing website or internal server in the middle of an incident, remediating immediately is usually not the best approach. Bear in mind, when you make these changes, you will also destroy the environment that was the scene of the crime, making it more difficult to answer questions about the data at risk, how much of your estate was exposed and what it was vulnerable to. Lacking that information will slow the incident response process so it is important to preserve the scene before patching anything.
3. **Quick, pull the plug!** You can't be hacked without power. Very true. However most of the information you will need to answer questions about an attack reside in live system memory. Without this information, questions such as the following will be difficult for the incident responders to answer:
   - What was the malware connecting to internally and externally?
   - What credentials were at risk?
   - How long has this attack been occurring?
   - Is it active right now?

   If it's not ransomware, attackers can do little with malware they can't control so think twice before pulling plug in an effort to contain the attack.

4. **Moving / copying malware**: When IT teams do find malicious files and malware on their systems, a common approach is to move it to a folder on their desktop called “malware” while using the infected system to do some backyard malware analysis. This usually results in the loss of important information regarding where the malware originated including date and time stamps, all whilst the still active attacker watches the IT team attempt to figure out what happened.
5. **Uploading malware to Virus Total:** Virus Total is fantastic. However, when you upload malware to this and other sandbox services, the files are available for anyone else on that platform to download, tipping off the world as to what malware was active on your systems. Moreover, attackers usually monitor for when their malware has been uploaded to Virus Total as an early warning sign that you are on to them. Rather use the search function or switch to offline or private malware analysis sandboxes.
6. **Immediately blocking C2 channels:** Blocking Command and Control (C2) channels is an important aspect of incident containment; however, it must be executed at the right time. Often the right time is not immediately once you’ve found it, as attackers can and often do have multiple C2 Channels. Blocking the C2 channels carries the risk of alerting the attackers, causing them to change their behaviour and start creating more channels in increasingly obscure ways or to become destructive. This will make it more challenging for incident response to get ahead of the attack. As such, make sure you balance having sufficient intelligence on the attack with the data leakage risk before deciding to block C2 channels.
7. **The “Just rebuild it” approach:** When you rebuild a system, you lose almost all data about the attack, and will likely re-introduce the security risks that got it compromised in the first place. If you are in the middle of a major incident, any system being rebuilt is worth preserving first in case an investigation is needed. In normal day to day incident management, the same rule applies. Finding out that the source of an attack was a workstation you had in fact rebuilt is a hapless scenario as questions about how or what occurred will remain unanswered. Worse you can end up playing ‘whack-a-mole’ with the attacker as they repeatedly re-establish a beach head using the same attack vectors.
8. **There’s no space, delete the logs:** Operational IT and security teams need to work hand in glove when an incident is underway. Often, operations teams will help carry out instructions to move large amounts of data around for analysis. Usually, when space is limited, these teams will delete what they believe to be valueless data such as logs. In fact, these are exceptionally valuable to the incident investigation. Make sure your security and operations teams have first responder training and know what you are trying to achieve so that valuable data is not lost.
9. **It must be an insider!** Attribution is a common request we receive from clients. Security teams believing an insider must be to blame is a common hindrance to the incident response process. The belief that you couldn’t have been hacked from outside is a natural one and this normally leads to looking internally. However, the administrators and managers of compromised systems who have the knowledge of how these systems work and what might have happened are the people you now suspect. Being on the wrong side of these individuals can obstruct an efficient investigation. Whilst insider threats are real, the vast majority are perpetrated from outside the organisation or the country, where local law enforcement cannot reach them. Un-authorised

privileged account use is an expected attacker behaviour. Be observant, keep an open mind, but keep your internal team's on-side until you have the full picture.

10. **Assuming the best:** By far, this is the most common mistake security and response teams make: assuming the attacker did not use their access as leverage to move laterally towards their goal. Unless you have caught an incident early at the point of entry, assume the worst, it is safer in the long run. Look at what an attacker could have done, and where they could have moved. Test those theories to prove the worst did not happen. Our experience shows that assuming the best-case scenario, usually leads to the worst-case results.

13 Appendix C - Content Checklist

The table below shall demonstrate how the policy addresses the key relevant regulatory requirements and guidelines:

General Policy Guideline			
	Content Requirement	**Source**	**Addressed**
1	The policy must be aligned with all other policies and with the company's business strategy.	EIOPA 2015 Final Report on Public Consultation No. 14/017 on Guidelines on system of governance Guideline 7	Aligned
2	Set out the goals pursued by the policy	EIOPA 2015 Final Report on Public Consultation No. 14/017 on Guidelines on system of governance Guideline 7(a)	1.1
3	Set out the tasks to be performed and the person or role responsible for them	EIOPA 2015 Final Report on Public Consultation No. 14/017 on Guidelines on system of governance Guideline 7(b)	3.4
4	Set out the processes and reporting procedures to be applied	EIOPA 2015 Final Report on Public Consultation No. 14/017 on Guidelines on system of governance Guideline 7(c)	3.4, 4.6 & 5
5	Set out the obligation of the relevant organisational units to inform the risk management, internal audit, compliance and actuarial functions of any facts relevant for the performance of their duties.	EIOPA 2015 Final Report on Public Consultation No. 14/017 on Guidelines on system of governance Guideline 7(d)	6
6	If the policy relates to a key function, it should also address the position of the function within COMPANY, its rights and powers.	EIOPA 2015 Final Report on Public Consultation No. 14/017 on Guidelines on system of governance Guideline 7	n/a
Cybersecurity Policy			
	With regard to cybersecurity, the Central Bank expects that:	CBI's Cross Industry Guidance in respect of Information Technology and Cybersecurity Risks 3. Cybersecurity	**Addressed**
7	1. Cyber risk is managed within the context of overall IT risk management.		4
8	2. Firms have a well-considered and documented strategy, reviewed and approved by the Board, in place to address cyber risk. Documented cybersecurity policies and procedures are maintained, monitored and enforced which support effective implementation of the security risk management strategy. Cybersecurity roles and responsibilities are clearly defined, documented and communicated to relevant staff.		2, This Policy, & 9
9	3. Firms develop and implement security awareness training programmes to provide information on good IT security practices, common threat types and the firm's policies and procedures regarding the appropriate use of applications, systems and networks. Staff with privileged access rights, in particular, should be aware of good IT security behaviour and all staff should have an appreciation of the importance of security to critical business activities and objectives.	Cross Industry Guidance in respect of Information Technology and Cybersecurity Risks 3. Cybersecurity	3; 4.5
10	4. At a minimum, cyber risk management addresses: - the identification of threats, vulnerabilities and risks and quantification of exposure specific to the firm; - the prevention and detection of security events and incidents, including reducing likelihood of occurrence and potential impact when it does;	Cross Industry Guidance in respect of Information Technology and Cybersecurity Risks 3. Cybersecurity	3 and 12

	- security incident handling; and - recovery planning for stabilisation and continuity of operations in the immediate aftermath of a security incident.		
11	5. Cyber risk assessments are performed on a regular basis and include identification of external and internal threats. To support intelligence gathering on current and emerging threats and vulnerabilities, firms should consider participating in security information sharing forums.	As Above	3; 4
12	6. Robust safeguards are in place to protect against cybersecurity events and incidents. Techniques and technologies that firms may consider include, but are not limited to, strong authentication, encryption, intrusion prevention and detection, advanced malware protection, strong access controls (including physical controls) and network segmentation providing isolation and defence in depth when required.	As Above	3
13	7. There are processes in place to classify data enabling the firm to identify sensitive, valuable and critical data that the firm stores, processes or transmits. Appropriate safeguards (commensurate with the value or importance of the data) are implemented to ensure that it remains secure, complete, accurate and readily available to authorised users who need it. The processes should provide for the secure logging of all data access.	As Above	3 & Information Classification & Protection Policy
14	8. Firms implement strong controls over access to their IT systems, whether from inside or outside the firm. Users are granted only the level of access required to perform their responsibilities ("Principle of Least Privilege") and only staff with proper authorisation are permitted to access sensitive or critical data and systems.	As Above	3
15	9. Adequate processes are in place to monitor information systems and assets and to detect security events and incidents in a timely manner, preferably using predictive indicators. The effectiveness of detection processes and procedures are tested periodically. This can be achieved by conducting penetration testing exercises undertaken by either the firm's staff or trusted third parties.	As Above	3.2;3.3; 3.4
16	10. Firms have a documented cybersecurity incident response plan in place that provides a roadmap for the actions the firm will take during and after a security incident. Incident response plans address, inter-alia, the roles and responsibilities of staff, incident detection and assessment, reporting and escalation as well as response strategies to be deployed. A plan for communications with relevant external stakeholders, including customers, also forms a part of the response plan.	As Above	12
17	11. The firm notifies the Central Bank when it becomes aware of a cybersecurity incident that could have a significant and adverse effect on the firm's ability to provide adequate services to its customers, its reputation or financial condition.	As Above	6
18	12. A documented recovery plan is in place to resume critical operations rapidly following a cybersecurity incident. Key findings from the lessons learned from cybersecurity incidents are incorporated into the refinement and update of control structures and the incident response and recovery plans.	As Above	12
19	13. Firms consider relevant good practices and internationally adopted frameworks for IT security risk management as may be appropriate for their firm.	As Above	9
20	**Guideline 2 – ICT within the system of governance**		

	10. The AMSB should ensure that the quantity and skills of the undertakings' staff is adequate to support their ICT operational needs, ICT and security risk management processes on an ongoing basis and ensure the implementation of their ICT strategy. Furthermore, staff should receive adequate training on ICT and security risks, including information security, on a regular basis, as set out in Guideline 13.	• Guidelines on Information and Communication Technology Security and governance EIOPA-BoS-20/601	4.5.1 and 4.5.2
	11. The AMSB should ensure that the allocated resources are appropriate to fulfil the above requirements.		
21	**Guideline 4 – ICT and security risks within the risk management system**		
	16. The AMSB has overall responsibility to establish effective system for managing ICT and security risks as part of the undertaking's overall risk management system. This includes the determination of the risk tolerance for those risks, in accordance with the risk strategy of the undertaking, and a regular written report about the result of the risk management process addressed to the AMSB.		4.1
	17. As part of their overall risk management system, undertakings should in relation to ICT and security risks (while defining the ICT protection requirements as described below) consider at least the following:		
	a) undertakings should establish and regularly update a mapping of their business processes and activities, business functions, roles and assets (e.g. information assets and ICT assets) in order to identify their importance and their interdependencies to ICT and security risks;		3.1
	b) undertakings should identify and measure all relevant ICT and security risks they are exposed to and classify the identified business processes and activities, business functions, roles and assets (e.g. information assets and ICT assets) in terms of criticality. Undertakings should also assess the protection requirements of, at least, confidentiality, integrity and availability of those business processes and activities, business functions, roles and assets (e.g. information assets and ICT assets). Asset owners, who are accountable for the classification of the assets should be identified;		3.1 and 4
	c) the methods used to determine the criticality as well as the level of protection required, in particular with regard to the protection objectives of integrity, availability and confidentiality, should ensure that the resulting protection requirements are consistent and comprehensive;		3.1
	d) the measurement of ICT and security risks should be conducted on the basis of the defined ICT and security risk criteria taking into account the criticality of their business processes and activities, business functions, roles and assets (e.g. information assets and ICT assets), extent of known vulnerabilities and prior incidents that impacted the undertaking;		4
	e) the assessment of ICT and security risks should be carried out and documented regularly. This assessment should also be performed ahead of any major change in infrastructure, processes or procedures affecting the business processes and activities, business functions, roles and assets (e.g. information assets and ICT assets);		4
	f) based on their risk assessment undertakings should, at least, define and implement measures to manage identified ICT and security risks and protect information assets in accordance with their classification. This should include the definition of measures to manage the remaining residual risks.		4

	18. The results of the ICT and security risk management process should be approved by the AMSB and included in the process of operational risk management as part of the undertakings' overall risk management.		4
22	**Guideline 5 - Audit**		
	19. Undertakings' governance, systems and processes for its ICT and security risks should be audited on a periodic basis in line with the undertakings' audit plan by auditors with sufficient knowledge, skills and expertise in ICT and security risks to provide independent assurance of their effectiveness to the AMSB. The frequency and focus of such audits should be commensurate with the relevant ICT and security risks.		4.6.1
23	**Guideline 6 – Information security policy and measures**		
	20. Undertakings should establish a written information security policy approved by the AMSB which should define the high-level principles and rules to protect the confidentiality, integrity and availability of undertakings' information in order to support the implementation of ICT strategy.		This Policy
	21. The policy should include a description of the main roles and responsibilities for information security management, and it should set out the requirements for staff, processes and technology in relation to information security, recognising that staff at all levels have responsibilities in ensuring undertakings' information security.		7.2
	22. The policy should be communicated within the undertaking and should apply to all staff. Where applicable and relevant, the information security policy or parts of it should also be communicated and applied to service providers.		7.3
	23. Based on the policy, undertakings should establish and implement more specific information security procedures and information security measures to, inter alia, mitigate the ICT and security risks they are exposed to. These procedures and information security measures should include every process described in these Guidelines, as applicable.		Initiatives, Projects, Tasks
24	**Guideline 7 - Information security function**		
	24. Undertakings should establish, within their system of governance and in accordance with the proportionality principle, an information security function, with the responsibilities assigned to a designated person. The undertaking should ensure the independence and objectivity of the information security function by appropriately segregating it from ICT development and operations processes. The function should report to the AMSB.		3.4
	25. The tasks of the information security function are typically to:		7.2
	a) support the AMSB when defining and maintaining the information security policy for undertakings and control its deployment;		
	b) report and advise the AMSB regularly and on an ad hoc basis on the status of information security and its developments;		
	c) monitor and review the implementation of the information security measures;		
	d) ensure that the information security requirements are adhered to when using service providers;		
	e) ensure that all employees and service providers accessing information and systems are adequately informed of the information security policy, for example through information security training and awareness sessions;		
	f) coordinate operational or security incident examination and report relevant ones to the AMSB.		

25	**Guideline 8 – Logical security**		
	26. Undertakings should define, document and implement procedures for logical access control or logical security (identity and access management) in line with the protection requirements, as defined in Guideline 4. These procedures should be implemented, enforced, monitored and periodically reviewed, and should also include controls for monitoring anomalies. These procedures should, at a minimum, implement the following elements, where the term 'user' also comprises technical users:		3.2 and Information Classification and Protection Policy
	a) need-to-know, least privilege and segregation of duties: undertakings should manage access rights, including remote access to information assets and their supporting systems on a 'need-to-know' basis. Users should be granted the minimum access rights that are strictly required to execute their duties (principle of 'least privilege'), i.e. to prevent unjustified access to data or that the allocation of combinations of access rights may be used to circumvent controls (principle of 'segregation of duties');		
	b) user accountability: undertakings should limit, as much as possible, the usage of generic and shared user accounts and ensure that users can be identified and traced back to a responsible natural person or an authorised task for the actions performed in the ICT systems at all times;		
	c) privileged access rights: undertakings should implement strong controls over privileged system access by strictly limiting and closely supervising accounts with elevated system access (e.g. administrator accounts);		
	d) remote access: in order to ensure secure communication and reduce risk, remote administrative access to critical ICT systems should be granted only on a need-to-know basis and when strong authentication solutions are used;		
	e) logging of user activities: users' activities should be logged and monitored in a risk proportionate manner, comprising, at a minimum, privileged users' activities. Access logs should be secured to prevent unauthorised modification or deletion and retained for a period commensurate with the criticality of the identified business functions, supporting processes and information assets, without prejudice to the retention requirements set out in EU and national law. Undertakings should use this information to facilitate identification and investigation of anomalous activities that have been detected in the provision of services;		
	f) access management: access rights should be granted, removed and modified in a timely manner, according to predefined routines for approval where the applicable information asset owner is involved. In case access is no longer required, access rights should be promptly revoked;		
	g) access assessment: access rights should be periodically reviewed to ensure that users do not possess excessive privileges and that access rights are withdrawn/removed when no longer required;		
	h) the granting, modification, revocation of access rights should be documented in a way that facilitates comprehension and analysis; and		
	i) Authentication methods: undertakings should enforce authentication methods that are sufficiently robust to adequately and effectively ensure that access control policies and procedures are complied with. Authentication methods should be commensurate with the criticality of ICT systems, information or process being accessed. This should, at a minimum, include strong passwords or stronger authentication methods (such as two-factor authentication), based on relevant risk.		

	27. Electronic access by applications to data and ICT systems should be limited to the minimum required to provide the relevant service.		
26	**Guideline 9 – Physical security**		3.2
	28. Undertakings' physical security measures (e.g. protection against power failure, fire, water and unauthorised physical access) should be defined, documented and implemented to protect its premises, data centres and sensitive areas from unauthorised access and from environmental hazards.		
	29. Physical access to ICT systems should be permitted only to authorised individuals. Authorisation should be assigned in accordance with the individuals' tasks and responsibilities and limited to individuals who are appropriately trained and monitored. Physical access should be regularly reviewed to ensure that unnecessary access rights are promptly withdrawn/removed.		
	30. Adequate measures to protect from environmental hazards should be commensurate with the importance of the buildings and the criticality of the operations or ICT systems located in these buildings.		
27	**Guideline 10 – ICT operations security**		3.2
	31. Undertakings should implement procedures to ensure confidentiality, integrity and availability of ICT systems and ICT services in order to respectively minimise the impact of security issues on ICT service delivery. These procedures should appropriately include the following measures:		
	a) identification of potential vulnerabilities which should be evaluated and remediated by ensuring that ICT systems are up to date, including the software provided by undertakings to its internal and external users, by deploying critical security patches, including antivirus definitions updates or by implementing compensating controls;		
	b) implementation of secure configuration baselines for all critical components such as operating systems, databases, routers or switches;		
	c) implementation of network segmentation, data leakage prevention systems and the encryption of network traffic (in accordance with the information asset classification);		
	d) implementation of protection of endpoints including servers, workstations and mobile devices. Undertakings should evaluate whether an endpoint meets the security standards defined by them before it is granted access to the corporate network;		
	e) ensuring that integrity-checking mechanisms are in place to verify the integrity of ICT systems;		
	f) encryption of data at rest and in transit (in accordance with the information asset classification).		
28	**Guideline 10 – ICT operations security**		3.2
	31. Undertakings should implement procedures to ensure confidentiality, integrity and availability of ICT systems and ICT services in order to respectively minimise the impact of security issues on ICT service delivery. These procedures should appropriately include the following measures:		
	a) identification of potential vulnerabilities which should be evaluated and remediated by ensuring that ICT systems are up to date, including the software provided by undertakings to its internal and external users, by deploying critical security patches, including antivirus definitions updates or by implementing compensating controls;		
	b) implementation of secure configuration baselines for all critical components such as operating systems, databases, routers or switches;		

	c) implementation of network segmentation, data leakage prevention systems and the encryption of network traffic (in accordance with the information asset classification);		
	d) implementation of protection of endpoints including servers, workstations and mobile devices. Undertakings should evaluate whether an endpoint meets the security standards defined by them before it is granted access to the corporate network;		
	e) ensuring that integrity-checking mechanisms are in place to verify the integrity of ICT systems;		
	f) encryption of data at rest and in transit (in accordance with the information asset classification).		
29	**Guideline 11 – Security monitoring**		3.2
	32. Undertakings should establish and implement procedures and processes to continuously monitor activities that impact the undertakings' information security. The monitoring should cover, at least:		
	a) internal and external factors, including business and ICT administrative functions;		
	b) transactions by service providers, other entities and internal users; and		
	c) potential internal and external threats.		
	33. Based on the monitoring the undertakings should implement appropriate and effective capabilities for detecting, reporting and responding to anomalous activities and threats, like physical or logical intrusion, breaches of confidentiality, integrity and availability of information assets, malicious code and publicly known vulnerabilities for software and hardware.		
	34. The reporting from the security monitoring should help the undertakings to understand the nature of both operational or security incidents, to identify trends and to support the undertakings' internal investigations and enable them to make appropriate decisions.		
30	**Guideline 12 – Information security reviews, assessment and testing**		
	35. Undertakings should perform a variety of different information security reviews, assessments and testing, so as to ensure effective identification of vulnerabilities in its ICT systems and services. For instance, undertakings may perform gap analysis against information security standards, compliance reviews, internal and external audits of the information systems, or physical security reviews.		3.4; 4.6.1
	36. Undertakings should establish and implement an information security testing framework that validates the robustness and effectiveness of the information security measures and ensure that this framework considers threats and vulnerabilities, identified through threat monitoring and the ICT and security risk assessment process.		
	37. Testing should be carried out in a safe and secure manner and by independent testers with sufficient knowledge, skills and expertise in testing information security measures.		5.1
	38. Undertakings should perform tests on a regular basis. The scope, frequency and method of testing (such as penetration testing, including threat led penetration testing) should be commensurate with the level of risk identified. Testing of critical ICT systems and vulnerability scans should be performed annually.		

	39. Undertakings should ensure that tests of security measures are conducted in the event of changes to infrastructure, processes or procedures and if changes are made because of major operational or security incidents or due to the release of new or significantly changed critical applications. Undertakings should monitor and evaluate results of the security tests and update their security measures accordingly without undue delays in case of critical ICT systems.		
31	**Guideline 15 - ICT incident and problem management**		Appendix B; IT Incidents reporting Process; Operational Risk Policy
	49. Undertakings should establish and implement an incident and problem management process to monitor and log operational or security incidents and enable undertakings to continue or resume critical business functions and processes when disruptions occur.		
	50. Undertakings should determine appropriate criteria and thresholds for classifying an event as an operational or security incident, as well as early warning indicators that should serve as an alert to enable early detection of these incidents.		
	51. To minimise the impact of adverse events and enable timely recovery, undertakings should establish appropriate processes and organisational structures to ensure a consistent and integrated monitoring, handling and follow-up of operational and security incidents to ensure that the root causes are identified, treated, and corrective actions/measures are taken to prevent the incident from happening again. The incident and problem management process should, at least, establish:		
	a) the procedures to identify, track, log, categorise and classify incidents according to a priority defined by the undertaking and based on business criticality and service agreements;		
	b) the roles and responsibilities for different incident scenarios (e.g. errors, malfunctioning, cyber-attacks);		
	c) a problem management procedure to identify, analyse and solve the root cause behind one or more incidents; undertakings should analyse operational or security incidents that have been identified or have occurred within and/or outside the organisation, and should consider key lessons learned from these analyses and update the security measures accordingly;		
	d) effective internal communication plans, including incident notification and escalation procedures - covering also security-related customer complaints - to ensure that:		
	i. incidents with a potentially high adverse impact on critical ICT systems and ICT services are reported to the relevant senior management;		
	ii. the AMSB is informed on an ad-hoc basis in case of significant incidents and at least informed of the impact, reaction and additional controls to be defined because of the incidents.		
	e) incident response procedures to mitigate the impact related to the incidents and to ensure that the service becomes operational and secure in a timely manner;		
	f) specific external communication plans for critical business functions and processes in order to:		
	i. collaborates with relevant stakeholders to effectively respond to and recover from the incident;		
	ii. provide timely information, including incident reporting, to external parties (e.g. customers, other market participants, relevant (supervisory) authorities, as appropriate and in line with applicable regulation).		