An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

Public Sector Cyber Security Baseline Standards

November 2021

Revision 1 November 2022

Prepared by the Department of
the Environment, Climate and Communications
gov.ie

Table of Contents

Executive Summary

The National Cyber Security Strategy 2019-2024 states that the National Cyber Security Centre (NCSC), in conjunction with the OGCIO, will under Measure 8 formulate a cyber security baseline standard for Government ICT. The Baseline Standard will be aligned with international standards and phased in across all **Public Service Bodies (PSBs)**. These standards typically include measures and controls in relation to staff training, identity and access management. Compliance with the standard which will be adhered to at local PSB level with support and guidance provided by the NCSC.

In order to effectively address the multiple public sector Information and Communications Technology (ICT) challenges and to improve the resilience and security of public sector ICT systems, a series of measures will be set out to develop and deploy a Cyber Security Baseline Standard to be applied to Government ICT systems and services. The recommendation of the Steering Group is that the Cyber Security Baseline Standards would apply to all Public Service Bodies.[1] The process for drawing up the standards was managed by a Steering Group with representation from stakeholders in Government Departments and agencies.

As part of the implementation framework of the Cyber Security Baseline Standards, the National Cyber Security Strategy proposed under Measure 10 of the Strategy to set up a Government IT Security forum for the implementation of the Cyber Security Baseline Standards across Government networks and Services. The Government IT Security forum will be created, open to all Heads of IT Security across Government, to facilitate information sharing on best practice for cyber security and to allow the NCSC to support the deployment of the baseline security standard.

The Steering Group insist that this standard is essential and will contribute in a positive way to foster a culture of cyber security and best practice across Public Service Bodies. Similar to practices in the aviation and healthcare industries, the Steering Group want to nurture a Cyber Security environment where every "identified risk" is seen as an opportunity to strengthen the system. This will help to remove a cyber security blame culture and positively reinforce cyber security best practices.

The positive contribution and involvement of Public Service Bodies in the Steering Group is essential in order to ensure that the design and implementation of Cyber Security Baseline

1 www.cso.ie

Standards are fit for Public Service ICT purposes and can demonstrate Cyber Security best practice.

Terms of Reference (ToR)

The National Cyber Security Strategy Baseline Measures will provide the mandatory protective security outcomes that all Public Service Bodies are required to achieve. The result will define the security measures that Public Service Bodies shall implement to improve the resilience and security of public sector ICT systems to better protect data and the services that our people rely upon. The Government IT Security forum will be a key factor in the deployment of the Cyber Security Baseline Standards for Public Service ICT purposes.

Within this document the terms:

- '**must**', '**will**' and '**shall**' mean that the detail is **mandatory**
- '**may**', '**should**' and '**could**' mean the detail is **discretionary**

In line with Measure 8 of the National Cyber Security Strategy, the Baseline standards typically include measures and controls in relation to staff training, identity and access management. Training should be provided within the public service system on the basic elements of Cyber Security. This approach will help to maximize existing resources as well as providing an opportunity for existing staff to develop Cyber Security skills.

Scope

The Public Service Cyber Security Baseline Standards Steering Group have presented a set of measures which are intended to create an acceptable security standard which can be revised over time to address new threats and vulnerabilities and to keep pace with new technologies and suppliers. The Cyber Security Baseline Standards shall apply to all Public Service Bodies.

Baseline Standards

The Baseline Standards are intended to create an acceptable security standard and form a broad framework for a set of measures which can be revised over time. The Baseline Standards model follows a holistic and comprehensive approach to the issues related to Cyber Security which combines the best of various standards to address the needs of key stakeholders.

Baseline Cyber Security Standards align with the NIST Framework[2]

NIST Cyber Security Framework				
Identify	**Protect**	**Detect**	**Respond**	**Recover**
• Asset Management • Business Environment • Governance • Risk Assessment • Risk Management Strategy	• Access Control • Awareness and Training • Data Security • Info protection Processes and Procedures • Maintenance • Protective Technology	• Anomalies and events • Security Continuous Monitoring • Detection Processes	• Response Planning • Communications • Analysis • Mitigation • Improvements	• Recovery Planning • Improvements • Communications

The NIST 1.1 CSF is a framework of cyber security guidance published by the U.S. National of Institute of Standards and Technology and is available to download from their website.

It is designed as a comprehensive framework for businesses and organisations to identify, assess and address the cyber security risks they face. NIST encourages any organisation or sector to review and consider the Framework as a helpful tool in managing cybersecurity risks.

There is no single solution or fix when it comes to cybersecurity and protecting a Public Service Body. For instance, "Zero-day" attacks exploiting previously unknown software vulnerabilities are especially problematic. However, using the Cyber Security Baseline Standard Framework to assess and improve the management of cybersecurity risks should put Public Service Bodies in a much better position to identify, protect, detect, respond to, and recover from an attack, minimising damage and impact.

The Cyber Security Baseline Standard compromises of 5 different ‘’themes” that form a framework for the set of Baseline Measures. The themes are:

I. **Identify:** Understand the structures, policies and processes required to manage cybersecurity risk to systems, assets, data and capabilities.

II. **Protect:** Develop and implement the appropriate and proportionate cyber security measures to deliver and protect the organisations essential services and systems.

[2] https://www.nist.gov/cyberframework

III. **Detect:** Develop and implement the appropriate capabilities to identify, detect and defend against a cybersecurity event that may have the potential to affect essential services and systems.

IV. **Respond:** Develop and implement the appropriate activities, prioritised through the organisations risk management process to take action to contain and minimise the impacts relating to a cybersecurity event.

V. **Recover:** Develop and implement the appropriate capabilities, prioritised through the organisations risk management process, to restore essential services that were affected by a cybersecurity event.

1 Identify

Public Service Bodies Cyber Security Governance Processes

Section 1: Identify - Cyber Security Governance Processes		
1.1	**Corporate Responsibility**	**Guidance Notes**
1.1.1	There shall be clear lines of responsibility and accountability to a designated point of contact for cyber security information and systems.	It is essential that the organisation has clearly defined roles and responsibilities for managing cyber security. A designated point of contact must be nominated. The overall accountability for cyber security lies with an organisation's board of management.
1.2	**Management of ICT Security Policies and Processes**	**Guidance Notes**
1.2.1	There shall be appropriate management of ICT security policies and processes in place to direct the Public Service Bodies overall approach to cyber security.	A cyber security policy or policies are documents created to provide guidance with regards to the cyber security of an organisation's assets including data and ICT systems. The Cyber Security policy defines the rules of operation, any applicable standards and guidelines for permitted functionality. Policies should be supported by procedures for all ICT assets and processes.
1.3	**Identify and Manage ICT Security Risks**	**Guidance Notes**
1.3.1	Public Service Bodies shall identify and manage ICT security risks and use an appropriate risk management process, such as: • Identify the Risk. • Analyse the Risk. • Evaluate or Rank the Risk. • Treat the Risk. • Monitor and Review the Risk.	It is essential that the organisation has effective risk management processes in place to handle cyber security risks. These processes must Identify, Analyse, Evaluate, Treat, Monitor and Review risks on an ongoing basis. All Cyber Security risks to organisational operations, assets, and individuals must be identified and understood. All internal and external threats to an organisation (strategic, operational and tactical) and vulnerabilities must be identified, assessed and documented. Suppliers and third-party partners of ICT systems are often overlooked. All

		stakeholders, components, and services must be identified, prioritised, and assessed using a cyber supply chain risk assessment process. All Cyber Security risks must be evaluated and prioritised accordingly, and an agreed methodology shall be implemented to rate risks by impact and probability to determine the associated level of cyber security risk. A risk register must contain Cyber Security risks and must be maintained and reviewed regularly. The risk register should contain all relevant information for the organisation to successfully manage and treat cyber security risks.
1.4	**Cyber Awareness Training**	**Guidance Notes**
1.4.1	Public Service Bodies shall ensure that relevant staff receive ongoing appropriate Cyber Security Baseline Standards training as well as guidance on cyber security.	For organisations with access to the One Learning platform, training material will be made available in Cyber Security related matters. For Example, a self-paced introduction to Cyber Security is available such as an Introduction to Cyber Security Awareness to all staff with appropriate access. In association with the NCSC and other Government bodies and agencies, Ongoing guidance on Cyber Security will be continuously provided via the One Learning platform. Cyber security baseline standards training will be made available and updated on an ongoing basis.
1.4.2	Mandatory Cyber Security awareness training and education must be provided by Public Service Bodies.	To aid with cyber security defence, organisations must provide cyber security awareness training and education for staff. All staff must receive appropriate awareness education and training as well as regular updates in organisational policies and procedures, as relevant for their roles. Awareness training should be ongoing, planned and may be delivered in different forms to include classroom based, web based, distance learning, self-paced, other, as appropriate.
1.5	**System Information - Public Service Bodies Shall Know and Record**	**Guidance Notes**

1.5.1	The organisation must categorise what systems are essential to the functioning of the organisation. Including what information is important for the running of the organisation, understand the impact of its loss, it's compromise or it's disclosure.	Organisations must identify, record and protect the confidentiality, integrity and availability of the information they hold or process. Risk assessments to determine the impact of the loss, compromise or disclosure should be conducted. The requirement for users to access sensitive data or key operational services must be understood, documented and continually managed. Necessary controls such as backup and recovery should be implemented to ensure the confidentiality, integrity and availability of data.
1.6	**Managed Physical and Environmental Access Control**	**Guidance Notes**
1.6.1	A Physical and Environmental security Access Control Policy shall be in place and include processes and guidelines for comprehensive protection.	A Physical and Environmental security access control policy shall be defined, approved by management, published and communicated to employees and relevant external parties. Physical and Environmental Access permissions and authorisations are managed, incorporating the principle of least privilege, separation of duties, and continually revalidated.
1.6.2	Third-party dependencies – a register of third-party suppliers must be developed and maintained by Public Service Bodies.	It is essential that PSBs know who their third-party suppliers are and a register of the PSB third party suppliers, who will be required to successfully execute the DRP, is maintained. The Public Service Bodies third party register must be available during the recovery process and must be reviewed regularly and where possible, tested regularly.
1.6.3	All third parties must be made aware of the organisation's cyber security obligations.	Third parties are essential to the running of ICT systems. Organisation's must make third parties aware of their security obligations when attending the organisation premises or accessing its ICT systems.
1.6.4	Dependencies on third parties are recognised and recorded including:	Agreements with third parties should include requirements to address the cyber security risks associated with ICT services and the supply chain.

	• Third parties including sub-contractors and cloud service providers • Third-party supporting infrastructure e.g. power and communication links. • Contract relationships with third parties supporting critical activities, processes, services and infrastructure (including facilities) are properly documented and listed.	All relevant cyber security requirements should be established and agreed with each supplier that may access, process, store, communicate, or provide ICT infrastructure components for the organisation's information.
1.6.5	There is a clear and documented shared responsibility model between the organisation and suppliers/service providers	Organisations should continually monitor and review supplier service delivery. Cyber security requirements including shared responsibility for mitigating risks associated with supplier's access to ICT assets should be agreed with the supplier and documented.
1.7	**Key Operational and Essential Services**	**Guidance Notes**
1.7.1	Public Service Bodies shall know and record: • What their key operational and essential services are. • What technologies and services their operational services rely upon to remain available and secure.	It is essential that organisations identify and record what their key operational services and their dependencies on those services. Organisations must have well defined and tested procedures in place to ensure the continuity of key operational services in the event of failure of compromise. Technologies and services must be identified and protected.
1.7.2	What other dependencies operational services have. The impact arising from the loss of service availability. Appropriate access control procedures shall be in place to ensure that users only have access to systems that they have been approved to access and that are necessary for their role.	Third-party suppliers for the provision of services must be managed and through a formal process be continually reviewed. Risk assessments should be conducted to determine the impact arising from the loss of service availability. Results should be recorded, and the necessary controls implemented, where relevant. A formal backup procedure should be implemented for all ICT systems. Regular business continuity and disaster recovery tests should be conducted and

		restoring services to normal operation should be a well-practiced scenario.
1.7.3	Access control procedures shall be continually reviewed. Public Service Bodies must have an appropriate joiner, movers, leavers policy and third parties shall only have approved system access for the specific period of time necessary for their role.	Identities and credentials should be issued using the least privilege principle, managed, verified, revoked, for the joiner, movers and leavers lifecycle.
1.8	**Access Control Procedures**	**Guidance Notes**
1.8.1	Appropriate access control procedures shall be in place to ensure that users only have access to systems that they have been approved to access and that are necessary for their role.	An access control policy shall be defined, approved by management, published and communicated to employees and relevant external parties. The policy should be based on the principle of least privilege. The policy should include the security requirements of business applications, authorisation, consistency of the access rights and classification of systems, relevant legislation and contractual obligations regarding the limitation of access to data or systems, segregation of access control roles e.g., access request and access authorisation, removal of access rights, requirements for periodic review of access rights, roles with privileged access, audit records. The policy should be supported by procedures for access control of various ICT systems in the organisation.
1.8.2	Access control procedures shall be continually reviewed.	The Access Control Policy and procedures must be continually reviewed based on business and cyber security requirements.
1.9	**Joiner, Movers, Leavers Policy**	**Guidance Notes**
1.9	An appropriate joiner, movers, leavers policy shall be in place.	A joiner, movers, leavers policy shall be defined, approved by management, published and communicated to employees and relevant external parties. The policy should include details for revoking access when it is no longer required or changed for movers. The implementation of the policy demonstrates control of ICT assets and

		consequently aides with cyber security and financial due diligence.
1.9.2	Third parties shall only have approved system access for the specific period of time necessary for their role.	Third parties must be informed on their cyber security responsibilities prior to being granted access to ICT systems. Third party access must be approved based on their role and only be provided for the period required to complete their role. Third parties that require access to ICT systems must sign a non-disclosure agreement.

2 Protect

Public Service Bodies Shall Have in Place Appropriate Safeguards to Protect and Ensure Delivery of Critical Infrastructure Services

Section 2: Protect - Cyber Security Protection Processes		
2.1	**Access Control and Responsibility**	**Guidance Notes**
2.1.1	Access to information and services shall only be provided to authorised, known and individually referenced users or systems. Access permissions and authorisations are managed incorporating the principles of least privilege and separation of duties.	Access permissions and authorisations are managed, incorporating the principles of least privilege and separation of duties, and periodically revalidated. a. **Principle of Least Privilege:** The principle of least privilege states that an individual should be given the bare minimum access needed to perform their job functions. Users should only have the least amount of privileges required to perform their job and no more. This reduces authorisation exploitation by limiting access to resources for which they are not authorised. b. **Separation of Duties:** The principle of separation of duties states that no user should have all the privileges necessary to complete a critical business function. Beyond limiting user privilege level, you should also limit user duties, or the specific jobs they can perform. No user should be given responsibility for more than one related function. This limits the ability of a user to perform a malicious action and then cover up that action.
2.1.2	An Access Control Policy should be in place.	Is there an Access Control Policy? Access control policies are high-level documents that specify how access is managed and who may access information under what circumstances. NIST NISTIR 7316, Assessment of Access Control Systems explains some of the commonly used access control policies, models and mechanisms

		available in information technology systems, such as: • User access management • User registration and de-registration • User access provisioning • Management of privileged access rights • Management of secret authentication information of users • Review of user access rights • Removal or adjustment of access rights
2.1.3	Remote access is managed and documented.	Remote access is managed and documented. See NCSC Working From Home Security Advice 2020-04-08 Remote access control refers to the ability to monitor and control access to a computer or network anywhere and anytime. Are policies and procedures related to remote users' access permissions formalised? Are remote users (e.g., employees, contractors, third parties) access to critical systems approved and documented? Are remote connections encrypted? Are appropriate authentication mechanisms in place (e.g., multifactor, strong password parameters).
2.1.4	**For Information on MFA See Section 2.12**	
2.2	**Identification and Authentication**	**Guidance Notes**
2.2.1	Users shall always be identified prior to being provided access to information or services. Depending on the sensitivity of the information or criticality of the service.	Only individually authenticated and authorised users can connect to or access the organisation's networks or information systems. a. Access rights should be documented in accordance with appropriate NIST or ISO 27K standards. Users that can access personal data are appropriately authenticated.

		b. Both electronic and physical access requires individual authentication and authorisation.
2.2.2	Users shall always be authenticated prior to being provided access to information or services. Depending on the sensitivity of the information or criticality of the service.	Users are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the access (e.g., privileged, admin, root). a. Each user is authenticated using a unique username and strong password before being granted access to applications, computers and network devices. b. Where possible default passwords must be updated to a strong password prior to introduction to productions environments. c. Multi-factor authentication shall be used for access to enterprise level social media accounts. d. Two-factor authentication should be implemented for remote access to the network by employees, administrators, and third parties.
2.3	**Digital Resources – ICT Digital Resources**	**Guidance Notes**
2.3.1	To protect ICT resources and data, Public Service Bodies shall track and record all hardware and software assets using a dedicated Asset Register and keep hardware and software assets registers up to date.	To protect the organisation, the organisation needs to know all digital resources and ICT assets that are on the network. All digital resources and ICT assets must be recorded in an appropriate assets register. **Hardware:** All hardware on an organisations network should be known and recorded in an appropriate register which is continually reviewed and updated. **Software:** The organisation should maintain a register of all software in use in their organisation. In practical terms, if the organisation does not know what software is in use, they are unaware of what software to update. The register of software must be continually reviewed and updated in line with asset management policies.
2.3.2	Ensure that infrastructure assets are not vulnerable to cyber-attacks by	**Hardware:** All hardware on an organisations network shall be known

	regularly updating and patching devices. All Infrastructure assets must be protected with appropriate security updates, configuration and patching. Where this is not possible, a risk analysis and risk assessment shall be undertaken and, where appropriate, mitigations shall be approved, applied and documented.	and recorded in an appropriate register. All hardware must be patched and updated when updates become available. **Software:** Outdated software can put your business systems at risk and outdated software can contain a host of security vulnerabilities. Consequently, all software installed within the organisation must be patched and updated in line with the organisation's patching policy. All software must be recorded in an appropriate software asset register which is continually reviewed and updated. **Operating Systems:** Operating systems are also critical software that need to be updated in line with the organisation's patching policy. Where it is not possible to update or patch software or hardware, a risk assessment shall be undertaken and, where appropriate, mitigations shall be approved, applied and documented.
2.3.3	Obsolete devices should be removed from the network. Assets that cannot be updated and cannot be removed from the network must be secured appropriately to protect the asset.	Obsolete devices should be identified and removed from the network. Assets that cannot be updated and cannot be removed from the network must be risk assessed and secured appropriately to protect the asset. • Obsolete systems will pose a threat to the production environment because they cannot be patched or updated. A number of techniques can be used to protect these devices. • Move affected devices to a protected network behind a firewall. If possible, install anti-malware and intrusion detection products to the devices. If possible, ensure that the organisation has sufficient monitoring of the obsolete device to detect a compromise. • Reduce the likelihood of compromise by preventing obsolete devices from accessing untrusted content (effectively making it difficult for malicious content to reach the device and exploit it). • Reduce the impact of compromise by preventing access to sensitive data or

		services from vulnerable devices (so even if the devices are compromised, the damage will be minimised). It is highly recommended to implement a combination of these two approaches. In the long-term, replacing obsolete systems should be the goal.
2.3.4	As part of the procurement process and before installation, a risk assessment must be undertaken of new hardware and new software assets to ensure that these new systems don't pose a threat to the organisation.	The introduction of new software and systems can pose a threat to the organisation. Procurement must ensure that a risk assessment of new systems is completed before new systems and software are introduced to the production environment. Ideally new systems and software should be tested and evaluated with regard to cyber security in a non-production environment to ensure that they are secure.
2.3.5	Regular tests for the presence of known vulnerabilities or common configuration errors shall be undertaken. A vulnerability management plan must be developed and implemented to remediate vulnerabilities in a timely manner, commensurate with the risk	2.3.5 Undertake security vulnerability assessments to review and test for the presence of known vulnerabilities or common configuration errors. It is critical that the PSB carries out scans or reviews of it's hardware and software to identify vulnerabilities. When vulnerabilities are detected there should be a process in place to update, patch or remediate any vulnerabilities.
2.4	**Digital Resources – Identify/ Active Directory**	**2.4 Guidance Notes**
2.4.1	A valid backup of Active Directory, SYSVOL and GPO policies must be taken and held securely in the event of an incident. A backup process must be in place for Active Directory and must include "System State Backup".	Active Directory (AD) is a directory service used within Microsoft networks and domains. It is essential that AD is protected as it generally provides authentication for application and services. In the event of an incident it may be necessary to restore Active Directory to restore services. Having the ability to restore this service is essential to a successful recovery of services.
2.4.2	SYSVOL must also be backed up securely.	SYSVOL must also be backed up securely. System volume or SYSVOL is a shared location within a domain. SYSVOL is used to deliver policy and logon scripts to domain members.

2.4.3	A good and secure backup of all configured Group Policy Objects (GPOs) must also be taken.	Having a secure backup of the domain GPO is essential. See backup-gpo command on Microsoft for more information on this command.
2.4.4	Ensure that the Directory Services Restore Mode (DSRM) password is set to a known value, in the event that an authoritative or non-authoritative restoration is required.	The DSRM password will be required, in the event that an authoritative or non-authoritative restoration of the domain is needed. See: ntdsutil on Microsoft
2.5	**Digital Resources - Data**	**Guidance Notes**
2.5.1	Ensure that data is backed up and that backups are verified on a regular basis. Ensure that backups are not stored on media that is accessible by malware or by unauthorised accounts. Where possible, backups should be retained in a secure off-line system or media.	Having a good backup is essential to the data recovery process. A data recovery capability must be in place that includes a systematic approach to the backup of essential data. This should include a formal comprehensive backup and recovery plan, verification of backups means backups are valid, readable, and free of errors. There is periodic backup testing to verify data is accessible and readable.
2.5.2	Adopt an appropriate backup strategy such as 3-2-1 Backup. The 3-2-1 backup rule is a best practice because it ensures that there is a copy of the data no matter what happens. Multiple copies prevent losing the only copy of the data. Multiple locations ensure that there is no single point of failure and that any data is safe from disasters such as fires and floods.	Adopt an appropriate backup strategy such as 3-2-1 Backup. The 3-2-1 backup strategy simply states that there should be **3 copies of the data (the production data and 2 backup copies) on two different media types (disk and tape) with one copy off-site** for disaster recovery. Multiple copies prevent losing the only copy of the data. Multiple locations ensure that there is no single point of failure and that the data is safe from disasters such as fires and floods.
2.5.3	Understand when data backups are scheduled, the frequency and the type of backup to be undertaken as per business requirement, e.g., full or incremental	Understand when data backups are scheduled, the frequency and the type of backup to be undertaken as per recovery point objectives (RPO) or as per business requirement e.g., full or incremental.
2.6	**Digital Resources - Network**	**2.6 Guidance Notes**
2.6.1	Understand the PSB organisational network.	There are continual reviews and updates to technical knowledge about networks and information systems, such as documentation and network diagrams, and these are securely stored and available. There should be a change management process in place.

2.6.2	All Internal and external network IP address ranges within the PSB's control shall be documented.	Organisational IP ranges are known, recorded, and managed; DNS changes and queries are effectively managed.
2.6.3	Understand how traffic moves around the Public Service Bodies network and all points of ingress and egress.	Use Ingress and Egress filtering to monitor, control and restrict traffic entering or leaving the network. Understand how traffic moves around the network and all points of ingress and egress. Certain Services & Ports recommended to be Blocked. Certain Services and Ports need to be restricted. Each rule that allows network traffic to pass through the firewall (e.g., each service on a computer that is accessible through the boundary firewall) is subject to approval by an authorised individual and documented (including an explanation of the business need).
2.6.4	Maintain current network diagrams which fully document the data flow	There are continual reviews and updates to technical knowledge about networks and information systems, such as documentation and network diagrams, and these are securely stored. There should be a change management process in place.
2.6.5	In the event that digital (IT/ICT) services are outsourced, The Public Service Bodies shall understand and accurately record: • what security related responsibilities are devolved to the supplier	Where services are outsourced, it shall be clearly understood and accurately recorded which security related responsibilities remain with the organisation and which are performed on behalf of the organisation by the supplier(s).
2.6.6	If available to the PSB, join the NCSC sensor program to gain access to cyber threat updates and malware retro hunting capabilities.	Join NCSC sensor program to gain access to cyber threat updates and malware retro hunting capabilities. The NCSC sensor program is an invaluable resource to all Government Departments and key agencies. It is highly recommended that all stakeholders engage with the NCSC in relation to this initiative. The sensor will provide insights into the organisations DNS traffic and the organisation can avail of malware retro hunting capabilities.

2.6.7	Protect the Public Service Bodies network communications, Where possible utilise the Office of the Government Chief Information Officer (OGCIO) DNS Service to resolve DNS queries.	Contact Office of the Government Chief Information Officer (OGCIO) DNS Service to resolve DNS queries. To compliment the NCSC sensor program, where possible, Departments and key agencies can also avail of the OGCIO central DNS servers that provide an additional layer of protection to your organisation by filtering out unwanted and unsafe DNS traffic.
2.6.8	Where possible use TLS to transmit data across the network.	TLS protocols provide authentication, confidentiality, and data integrity protection between a client and server. TLS provides encryption for traffic that crosses an organisations network. Traffic that is not encrypted can be viewed by malicious actors and information can be stolen. Ensuring that clients and servers use TLS ensures that traffic cannot be viewed as it traverses networks.
2.7	**Digital Resources – Logging/ Auditing**	**Guidance Notes**
2.7.1	Implement network monitoring to get insights to what is on the PSB network and to raise alerts if anomalies occur on the network.	Network monitoring systems include software and hardware tools that can track various aspects of a network and its operation, such as traffic, bandwidth utilization, and uptime. These systems can detect devices and other elements that comprise or touch the network, as well as provide status updates. The monitoring capability should have the ability to identify unauthorised or accidental misuse of systems or data. It is able to tie specific users to suspicious activity.
2.7.2	Appropriate logging for the Public Service Bodies must be enabled to provide information to respond to network incidents and attacks	When designing a monitoring solution, it should be appropriate and proportionate to the context of the system, the threat that the PSB faces and the resources available to you. It is recommended that logging datasets are time synchronised, using an accurate common time source, so separate datasets can be correlated in different ways.
2.7.3	Backups of logs and audit information must be retained for a duration	Retain backups of logs and audits information for a period of time, rather than just have a single rolling backup as this does not provide adequate

	appropriate to the Public Service Body needs.	protection if an infection/damage isn't noticed before the backup is overwritten. Consider how long it may be before something is detected and ensure backups are kept for longer. The logging architecture has mechanisms, processes and procedures to ensure that it can protect itself from threats comparative to those it is trying to identify. This includes protecting the service itself, and the data within it.
2.7.4	Log data analysis and normalisation should only be performed on copies of the data keeping the master copy unaltered.	Log data analysis and normalisation is only performed on copies of the data keeping the master copy unaltered. Access to logging data is limited to those with business need and no others.
2.8	**Digital Resources – End point Devices**	**Guidance Notes**
2.8.1	To protect end point devices, Public Service Bodies shall: • Track, record and maintain a current Asset Register of end point devices.	All end point devices and their configuration must be tracked and recorded.
2.8.2	Ensure appropriate protections are applied to end point devices to prevent the introduction of malware or the unauthorised transfer of data with removable media.	Removable media and end point devices are automatically scanned for malware or malicious content when it is introduced to any system. All removable media is formally issued to individual users who are accountable for its use and safe keeping. Users must not use unofficial media, such as unencrypted USB drives. Sensitive information is encrypted at rest on removable media. Where removable media must be reused or destroyed, it shall be done securely with appropriate steps taken to ensure that previously stored information is not accessible.
2.8.3	Manage end user devices such that security policies can be applied, and controls can be exerted over software that interacts with sensitive information.	Management of end user devices includes installing and updating operating systems and application patches, managing user accounts, and maintaining up-to-date security. There must be an end user device management process coupled with comprehensive endpoint services.

2.8.4	Run operating systems and software packages which are in current vendor support. It is strongly recommended that out-of-date software (i.e. software that is no longer supported) is removed from computer and network devices that are connected to or capable of connecting to the internet.	Software running on computers and network devices must be kept up-to-date and have the latest security patches installed. It is strongly recommended that out-of-date software (i.e. software that is no longer supported) is removed from computer and network devices that are connected to or capable of connecting to the internet.
2.8.5	Have an active patch deployment procedure and process to enable the timely installation of critical updates and allow for urgent security vulnerabilities to be addressed promptly.	Specifically, software running on computers and network devices that are connected to or capable of connecting to the internet is licensed and supported (by the software vendor or supplier of the software) to ensure security patches for known vulnerabilities are installed in a timely manner (in line with PSB policies and/or automatically when they become available from vendors).
2.8.6	Test Patch Efficacy Security and Technical Review.	Newly Released Patches should initially be installed on test systems and Public Service Bodies should use other methods of test patch efficacy prior to release into the production environment, such as a vulnerability scanner that is independent from the patch management system.
2.8.7	Encrypt data at rest on mobile devices, laptops and removable media.	Is confidential data at rest secured (e.g., strong encryption as defined by industry best practices)? Implement cryptographic mechanisms to prevent unauthorised disclosure and modification.
2.8.8	Where possible, have the ability to remotely wipe an end user device and/or revoke end user access to a device where appropriate.	Where possible, have the ability to remotely wipe an end user device and/or revoke access end user access to a device where appropriate.
2.9	**Email Security**	**Guidance Notes**
2.9.1	To protect email, Public Service Bodies shall: Implement Transport Layer Security between sending and receiving email gateways.	Implementing Transport Layer Security uses an encryption protocol intended to keep data secure when being transferred over a network or between sending and receiving email gateways.
2.9.2	E-mail TLS Recommendations.	Sending and Receiving E-mail Types of TLS Implementation:

		a. TLS Preferred is highly recommended as the default email gateway setting to be used In most cases there will be an option to use preferred TLS on all connections. Using preferred TLS means the servers will try to create an encrypted connection but will send email unencrypted if they cannot. **b. TLS Required is optional** For domains that support TLS, it may be possible to choose TLS required. This enforces TLS between the organisations email gateway and the recipient. If the recipient gateway does not support TLS, the sending of the email will fail. It is advised to engage with the recipient organisation to test and validate the TLS between both organisations. If the organisation email gateway supports TLS, the sending organisation will usually attempt the delivery of email over TLS.
2.9.3	Implement Sender Policy Framework (SPF) records for email domains in order to make email spoofing more difficult.	In addition, Organisations may also decide to Implement Sender Policy Framework (SPF) as this gives the receiver of an email information on the sender email and how legitimate the provenance of the email.
2.9.4	Where email is being used to send sensitive information, ensure that attachments are protected with encryption or strong passwords and decryption passwords are shared with the recipient through a mechanism other than email e.g., SMS or voice call.	The use of Out of Band Channels is highly recommended in this instance. Passwords should always be communicated in a separate beacon. Any Sensitive files should always be encrypted with a secure password and shared with the recipient on a separate communications channel.
2.9.5	Where appropriate, have Domain-based Message Authentication Reporting and Conformance (DMARC), Domain Keys Identified Mail (DKIM).	DMARC is an email validation tool designed to detect and prevent email spoofing, Using the DomainKeys Identified Mail (DKIM) standard will help prevent spoofing on outgoing messages sent from your domain.

2.9.6	Where appropriate implement spam and malware filtering and enforce DMARC on inbound email.	Spam is one of the most intrusive ways cybercriminals try to introduce malware and viruses into corporate systems. Spam and Malware Protection keeps the inbound mailbox free of annoying and harmful spam. Where email is being used to send sensitive information, ensure that attachments are protected with encryption or strong passwords and decryption passwords are shared with the recipient through a mechanism other than email e.g., SMS or voice call.
2.10	**Secure Web and Infrastructure Configuration**	**Guidance Notes**
2.10.1	To protect electronic delivery of information including data and content across multiple platforms and devices such as web or mobile, Public Service Bodies shall: Ensure web applications are not susceptible to common security vulnerabilities, such as described in the top ten Open Web Application Security Project (OWASP) vulnerabilities.	2.10.1 The primary measures against vulnerabilities in Web applications are robust development and testing in line with commercial best practices, such as described in the top ten Open Web Application Security Project (OWASP) vulnerabilities.
2.10.2	Ensure Public Service Bodies infrastructure has been securely configured to manufacturer best practice. Where this is not possible, a risk analysis and risk assessment shall be undertaken and, where appropriate, mitigations shall be approved, applied and documented.	Document the underlying infrastructure is secure, including verifying that the infrastructure is maintained securely. Critical infrastructure assets are identified; threats evaluated, and proportionate security measures are in place. Ensure Public Service Bodies infrastructure has been securely configured to manufacturer's best practice. Where this is not possible, a risk analysis and risk assessment shall be undertaken and, where appropriate, mitigations shall be approved, applied and documented. Network assets shall be regularly maintained to ensure service continuity. Network assets shall be protected from power surges and failures. Dependencies on supporting infrastructure (e.g., power, cooling etc.) shall be identified and recorded. Equipment and devices on premise shall be sited to ensure

		protection from external and internal environmental risks (e.g., water ingress).
2.11	**User Account Protection**	**Guidance Notes**
2.11.1	Public Service Bodies must adopt a model of least privilege. Implement Role Based Access Control (RBAC).	Users should be provided with the reasonable minimum rights and permissions to systems, services and information that they need to fulfil their business role. For some accounts an additional authentication factor (such as a token) may be appropriate. Assign responsibility for undertaking management reviews of accounts and related privileges. Implement Role Based Access Control (RBAC). Strictly control the granting of highly privileged system rights, reviewing the ongoing need regularly. Highly privileged administrative accounts should not be used for high risk use.
2.11.2	All Passwords shall be governed by an appropriate password policy to manage and secure passwords.	All Passwords shall be governed by an appropriate password policy to manage and secure passwords. Where passwords are in use, they should be of sufficient length and complexity to make them very difficult to guess (including by artificial intelligent systems used to guess millions of passwords a second) – they should be changed on a regular basis, particularly for business-critical systems.
2.11.3	Use of Administrative accounts should be separated from User accounts.	Use of Administrative accounts should be separated from User accounts. Administrators should use normal accounts for standard business use.
2.11.4	System and Service accounts should be fully recorded as well as where the accounts are in use on systems.	Maintain a secure listing of users with administrative privileges for the services in scope.
2.11.5	Public Service Bodies must implement processes to remove old and user accounts that are no longer required.	User permissions are reviewed monthly and when people change roles via the joiners, leavers and movers process.
2.11.6	PSB must review privileged accounts on a defined schedule or following any incident e.g., weekly, monthly, 3 monthly basis.	PSB must review privileged accounts on a defined schedule or as per Joiners, Movers and Leavers policy. Highly privileged accounts should not be vulnerable to common cyber-attacks. Multi-factor authentication shall be used where technically possible. such as

		where administrative consoles provide access to manage cloud-based infrastructure, platforms or services. Where MFA is not appropriate or is not possible, a risk analysis and risk assessment shall be undertaken and, where appropriate, mitigations shall be approved at an appropriate level, applied and documented.
2.11.7	Log and analyse all administrative actions to identify any suspicious or abnormal behaviour.	Log and analyse all administrative actions to identify any suspicious or abnormal behaviour. This includes monitoring user activity in accordance with HR policy, particularly access to sensitive information and the use of privileged account actions. Investigate where activities are outside of normal, expected bounds (such as access to large amounts of sensitive information outside of standard working hours).
2.12	**Multi-Factor Authentication (MFA)**	**2.12 Guidance Notes**
2.12.1	Multi-Factor Authentication shall be used where available and where it is appropriate and technically possible, such as where administrative consoles provide access to manage cloud-based infrastructure, platforms or services. Other authentication measures or mitigation should be considered and implemented where MFA is not appropriate or possible. Where MFA is not appropriate or is not possible, a risk analysis and risk assessment shall be undertaken and, where appropriate, mitigations shall be approved at an appropriate level, applied and documented.	Multi-Factor Authentication, also known as MFA or two-factor authentication (2FA) or two step verification, is an extra layer of security for online services asking users for another piece of evidence in addition to their password. The key benefit of MFA is the need for a matching pair, rather than the inherent strength of the second factor. It involves using your username and password and one other piece of information. This other piece of information can come in various forms. It may be: • A one-time dynamically issued token. • A physical object in the possession of the user. • A physical characteristic of the user (biometrics). An additional piece of information that is only known to the user.
2.12.2	Multi-Factor Authentication (MFA) shall be used for access to corporate social media accounts.	Corporate social media accounts are the public face of organisations. MFA must be used to block brute force password attacks and to prevent against misuse if the password is inadvertently disclosed in public.

2.13	Administrator Training	Guidance Notes
2.13.1	Administrators of infrastructure such as, network, user end point devices, servers and security systems must be appropriately trained and, if available, certified to manage and maintain that infrastructure.	Administrators and accountable individuals must receive appropriate training and guidance on of infrastructure such as, network, user end point devices, servers and security systems and, if available, certified to manage and maintain that infrastructure. Administrators and Employees in security roles are encouraged to engage in Continual Professional Development formally validate their cyber security skills through recognised certifications and specialist training.
2.13.2	Administrators must be appropriately trained in cyber security and understand how to detect and remediate anomalies.	Administrators and accountable individuals must receive appropriate cyber security training and guidance on cyber security and risk management. Administrators and employees in cyber security roles are encouraged to develop and formally validate their security skills through recognised certifications and specialist training. The effectiveness of cyber security training and awareness activities is monitored and tested.
2.14	**Security by Design**	**Guidance Notes**
2.14.1	Public Service Bodies should adopt a security by design principle when designing or procuring systems or software.	Security should not be an afterthought when implementing new systems. Designing and building security into systems will make it more difficult for attackers to compromise those systems and their data. Well-designed systems will make the disruption of those systems more difficult and will leave the Public Service Bodies better placed to detect an attack or compromise.

3 Detect

Public Service Bodies Shall Detect Cyber Security Incidents

Section 3: Detect - Cyber Security Detection Processes		
3.1	**Event Capture**	**Guidance Notes**
3.1.1	In the event of a cyber security incident, Public Service Bodies shall capture adequate log information to assist with the investigation of the incident. **See Section 2.7 for logs**	When a cyber security incident occurs, attackers will leave event or log information behind them. Logs are a systems eyes and ears for what is going on and logs can be vital when trying to detect and recover from cyber security incidents. PSB should have appropriate levels of logging information. These logs should be retained for an appropriate period of time to assist with the detection of a cyber security attack. Most, if not all network connected devices contain critical logs that can be vital in detecting an attack or loss of information.
3.2	**Cyber Security Incidents**	**Guidance Notes**
3.2.1	Cyber security incidents must be reported as soon as possible to the NCSC mailbox CertReport CertReport@decc.gov.ie. All reports to the NCSC are treated as highly confidential and will not be disclosed to third parties.	Public Service Bodies must have an appropriate process in place to deal with a cyber security incident. If an PSB detects or suspects a cyber security incident this must be reported immediately to the NCSC mailbox CertReport CertReport@decc.gov.ie **Please note:** Your report will be dealt with in the strictest confidence.
3.3	**Log Retention Period Legal**	**Guidance Notes**
3.3.1	Public Service Bodies shall understand all logging information and hold log information for a duration appropriate to their data retention policy and in line with their legal obligations. **See Section 2.7 for logs**	It is essential that the PSB knows and understands what logging information they capture and hold. With bespoke logging information, this information must be clearly understood by the organisation. The retention of logging and event information must be governed by an appropriate retention policy, where logging information is generated on a cloud platform, an appropriate retention

		policy should be defined and applied on that platform.
3.4	**Log Retention Period Malicious Activity Detections**	**Guidance Notes**
3.4.1	Logs must be retained for an appropriate period as defined by the PSB in order to assist with the detection of malicious activity such as an advanced persistent threat (APT).	An advanced persistent threat is a stealthy threat actor, typically a nation state or state-sponsored group, which gains unauthorised access to a computer network and remains undetected for an extended period. Advanced Persistent Threats (APT) pose their own unique challenges when it comes to detection due to the amount of time they could persist on systems before they are found. APTs can be present on a system for months. Public Service Bodies should have appropriate levels of logging information. These logs should be retained for an appropriate duration to assist in the detection of a cyber security attack and in particular APTs. Most if not all network connected devices contain critical logs that van be vital in detecting an attack or loss of information. **Note:** If you suspect that you have detected an APT please report it immediately to the NCSC mailbox CertReport CertReport@decc.gov.ie. **Your report will be dealt with in the strictest confidence.** **Do not take any direct actions against an APT. The NCSC will provide guidance on how to proceed with the incident.**
3.5	**CNI Protection**	**Guidance Notes**
3.5.1	Public Service Bodies shall clearly document what infrastructure must be protected and the importance of it.	Critical National Infrastructure (CNI) can be defined as those assets and systems necessary for the delivery of the essential services upon which daily life depends and which ensure the state continues to function effectively. **Source:** Strategic Emergency Management Guideline Part 2, Para 26. of the Strategic Emergency Management Guideline

		describes a methodology to identify CNI and to determine its criticality. An inventory of CNI must be clearly documented in detail and: • Be kept up to date. • Assigned a level of importance or criticality. • Supporting infrastructure e.g. comms links, access control systems, power and cooling systems must be fully understood and documented. • Interdependencies between critical components must be fully understood and documented in detail.
3.6	**Monitoring Controls**	**Guidance Notes**
3.6.1	Public Service Bodies shall document what monitoring controls are in place in the organisation.	Has the impact of any anomalous activity been documented? The organisation must clearly understand what monitoring systems are in place. The monitoring controls in place in an organisation must be fully documented. Staff shall be appropriately trained to use these monitoring tools and understand any alerts raised.
3.7	**Anomalous Activity Detection**	**Guidance Notes**
3.7.1	Monitoring solutions shall evolve with the Public Service Bodies business and as technology changes, as well as changes to the threat landscape.	As services are expanded and enhanced, security monitoring must be a factor when designing or enhancing a system. This ensures that adequate logging and monitoring is in place and that no security gaps emerge with monitoring. The incident monitoring process tracks and documents information security incidents. There is an understanding of what abnormalities to look for that might signify malicious activities, e.g.: • Unusual patterns of network traffic (e.g., unexpectedly high traffic volumes, or traffic of an unexpected type etc).

		• Deviations from normal interaction with systems (e.g., user activity outside normal working hours or from unexpected locations). • 'Tell-tale' signs of attack, such as attempts to laterally move across networks, or running privilege escalation software. • The retrieval of large numbers of essential service design documents.

4 Respond

Public Service Bodies Shall Develop a Cyber Incident Response and Management Plan, with Clearly Defined Actions, Roles and Responsibilities

Section 4: Respond - Cyber Security Respond Processes		
4.1	**Incident Recording**	**Guidance Notes**
4.1.1	All Public Service Bodies shall have a CIRP (Cyber Incidence Response Plan) which clearly outlines the organisation's response to all Cyber Security incidents. The term "cyber incident response plan" refers to an organised approach to handling (responding to) cybersecurity incidents. Cyber Incident response (CIRP) should be executed in a way that mitigates damage, reduces recovery time, and minimises costs. The set of instructions an organisation uses to guide their incident response team when a security event (i.e., a security breach) occurs is the Incident Response Plan See Annex 3.	Incidents are recorded in line with established criteria, consistent with legal and regulatory requirements. A culture of Cyber Readiness must be adopted by the Public Service Bodies. Businesses should assume that a Cyber Security incident will most likely happen during the course. In this case a CIRP will be essential and use commonly known processes for dealing with any incident. There are six phases of Incidence Response: 1. **Preparation**: Preparing the security staff to handle potential incidents. This includes training, equipping, and practicing. 2. **Identification**: Detecting and deciding if an incident fulfils the conditions to be considered a security incident by the organisation, and its severity. The severity level will inform how quickly the incident needs to be handled and who it might need to be escalated to. 3. **Containment**: Containing the incident by isolating compromised systems to prevent future damage. 4. **Eradication**: Detecting the cause of the incident and eliminating the threats from affected systems. 5. **Recovery**: Restoring affected systems and making sure no threat remains. 6. **Lessons Learned**: Analysing the incident logs, updating the

		response plan, and completing the incident documentation.
4.2	**Communications Plans**	**Guidance Notes**
4.2.1	Public Service Bodies shall have communication plans that are linked to the Cyber incident response and management plan in the event of an incident.	In the event of a cyber security incident, is the PSB ready to comply with regulatory reporting requirements? If the incident is under the Network and Information Security Directive. Please see the NCSC NIS Directive page. The communications plan must clearly record all stake holders with whom communications must be maintained during and incident. The plan must also ensure that a senior member of the communications team is part of the Cyber Incident Response Team. The contact details (including out of hours) in the event of compromised communications infrastructure) of all stakeholders must be documented, be available in paper and electronic format and reviewed regularly to ensure the currency of the contact information. The plan should also clearly document what communications are appropriate to use during and an incident (alternative mechanisms should be identified). In some circumstances, it may be prudent to establish a cloud-based communications system to reach stakeholders if primary communications channels are disabled during a cyber-attack. It is essential that the organisation has a communication plan ready to use in the event of a Cyber Security incident.
4.3	**Data Obligations**	**Guidance Notes**
4.3.1	Where a breach is likely to have resulted in a data breach this must be notified to the Public Service Bodies Data Protection Officer (DPO) without undue delay in line with GDPR regulation. Where a breach is likely to result in a high risk to the affected individuals, Public Service Bodies must also inform those individuals without undue delay.	If a Cyber Security Incident is known to have led to a data breach or data loss, this must be notified to your organisation's DPO without undue delay in line with the requirement of GDPR.

	https://www.dataprotection.ie/en/organisations/know-your-obligations/breach-notification	
4.4	**Cyber Incident Response Plan Review**	**Guidance Notes**
4.4.1	The cyber incident response plan must be reviewed and tested at regular intervals to ensure that all parties understand their roles and responsibilities as part of the plan. Post testing findings should inform the immediate future technical protection of the system or service, to ensure identified issues cannot arise in the same manner again. Systemic vulnerabilities identified shall be remediated and tested.	Cyber Incident Response Plan. **See Annex 3.** Information is shared consistent with response plans. When a Cyber Security Incident occurs, all plans will be tested and some areas of the plan may fail. The efficacy of the plans must be reviewed, and plans must be continually updated to include the lessons learned from the incident. Where systemic vulnerabilities have been identified, action must be taken to remediate these vulnerabilities as soon as possible.
4.5	**Mitigation Measures on Detections**	**Guidance Notes**
4.5.1	On discovery of an incident, mitigating measures shall be reported, assessed and applied at the earliest opportunity, drawing on expert advice where necessary.	When a cyber security incident occurs, a PSB may be required to act quickly to prevent an impact on production environments. All actions appropriate to the organisation will be detailed in a CIRP. These may include applying patches, making configuration changes, applying remediations and taking systems offline to protect them. It is critical that all action undertaken during an incident is fully documented and reviewed post-incident. During a "time critical event" such as human controlled malware, expert advice should be sought as soon as possible. Please note: A Cyber Security incident should be reported to certreport@decc.gov.ie as soon as the incident is detected.
4.6	**Post-Incident Sharing**	**Guidance Notes**
	Post-Incident, mitigation measures may be shared confidentially, and a collection of evidence shall be maintained as appropriate and in line with any legal obligations.	When an incident occurs, steps are taken to understand its root causes and ensure appropriate remediating action is taken to improve security. It may also be necessary to share information relevant to an incident with

		service providers, anti-malware vendors and the NCSC. If the PSB does not have an information classification policy, consider sharing information based on the Traffic Light Protocol. **TLP:RED** = Not for disclosure, restricted to participants only. **TLP:AMBER** = Limited disclosure, recipients can only spread this on a need-to-know basis within their organisation and its clients. **TLP:AMBER+STRICT** restricts sharing to the organisation only **TLP:GREEN** = Limited disclosure, restricted to the community. **TLP:CLEAR** = Disclosure is not limited.
4.7	**Post-Incident Lessons Learned**	**Guidance Notes**
	Post-cyber incident, a formal review shall be conducted, and lessons learned shall be added to the cyber incident response plan.	Recovery planning and processes are improved by incorporating lessons learned into future activities. It is highly advisable that all stakeholders involved in the management of an incident attend a formal review of the incident. A review can provide invaluable insights into how effective the Public Service Bodies CIRP was implemented.

5 Recover

Identify and Test Contingency Mechanisms

Section 5: Respond - Cyber Security Recover Processes		
5.1	**Recovery Points**	**Guidance Notes**
5.1.1	Public Service Bodies shall understand and define Recovery Points Objectives (RPOs) for all systems that need to be recovered. RPOs are the point in time where data is backed up in the most usable format and will be required for a recovery process.	A Recovery Point Objective (RPO) is defined within Business Continuity Planning (BCP). RPO is measured in time and is the maximum tolerable amount of data that can be lost when recovering from a disaster or failure. An RPOs determines the maximum age of the data or files in backup storage needed to be able to meet the objective defined by the RPO. For example, within the organisation, the RPO of 24 hours has been agreed by management as the tolerable point for loss of data during a disaster. If the last available good backup of data is from 20 hours ago, then the backup it is still within the timeframe of 24 hours set by the Business Continuity Plan's RPO.
5.2	**Disaster Recovery Plan (DRP)**	**Guidance Notes**
5.2.1	A Disaster Recovery Plan (DRP) must be in place for any Cyber Security Incident, such plans should also be in place with relevant suppliers. A DRP will define how Public Service Bodies will restore system access in a defined time period and will be informed based on the other four themes of the Baseline Security Standard. The following mandatory minimum items must be included in DRPs:	In the event of a Cyber Incident it is essential that Public Service Bodies have a plan to deal with an incident. An Incident Response Plan (IRP) ensures that in the event of a cyber security incident, the right personnel and processes are in place to effectively deal with a network cyber security incident. An IRP is essential and provides a targeted response to contain and remove the threat. An effective IRP is, a plan incorporating people, process and technology that is well documented, available during an incident and tested regularly. For more information see: Incident management A Disaster recovery Plan (DRP) differs from an IRP and ensures that in the event of a disaster that the right teams and processes are in place to effectively deal with the disaster. A DRP allows

		organisations to respond immediately to reduce damage and resume core business functions as quickly as possible. An effective DRP is, a plan incorporating people, process and technology that is well documented, available during a time of disaster and tested regularly. For more information see: Guide for Cybersecurity Event Recovery and Disaster management **Note:** It is essential that Incident Response and Disaster Recovery plans are linked to the organisations business continuity and crisis management plans, and fully supported with the necessary resources for the functions.
5.2.2	Service Level Agreements (SLA) or Memorandum of Understanding (MOU) – with details of response and recovery times guaranteed by suppliers.	Where possible, SLAs or MOUs should be established with reference to the priority of service restoration. It is essential for the PSB to establish clear and measurable response and recovery objectives in an SLA/MOU that is agreed between the PSB and its service providers. SLAs/MOUs ensure that the service provider will meet the Public Service Bodies specific needs. The Public Service Bodies set of SLAs/MOUs must be documented and reviewed regularly.
5.2.3	Authority – details for two or more senior personnel with the authority to activate the plan.	The DRP must clearly record the senior individuals who have responsibility to activate the DRP. The details of these senior individuals must be documented, be available during an incident and be reviewed regularly to ensure the currency of the contact information.
5.2.4	Recovery team membership – contact details for personnel responsible for implementing the DRP.	In the event of a major incident, recovery teams will be required. The DRP must clearly record the team members required to execute the DRP. The contact details of team members must be documented, be available during a time of disaster and reviewed regularly to ensure the currency of the contact information.
5.2.5	Specific recovery details and procedures – detailed plans on how to recover systems based on each Public Service Bodies specific systems and requirements. This will	Each PSB has its own set of specific recovery objectives. Organisations must maintain a set of recovery procedures that will be executed during a recovery scenario. The document should be clearly available to teams when required and

	be based on the Recovery Points as detailed in 5.1 Recovery Points.	must be regularly tested to ensure that they remain effective.
5.2.6	Out of band communications – methods of communications that do not rely on production systems used by Public Service Bodies .	In the event that production systems are not available, Public Service Bodies will require an out of band communication channel to coordinate recovery actions. This channel should be decided and contact details for all teams must be recorded and regularly reviewed.
5.2.7	Communications plan – details on how to communicate with internal and external stakeholders during the recovery process. This should include press offices, where relevant.	A communications plan must be available to the PSB to provide updates to manage and customer while business systems are recovered. The communications plan should include: • the details of all personnel required to respond to an incident • a means to contact all stakeholders impacted by an outage • clearly document the out of band communication channel • the plan must be linked with the DRP and IRPs
5.2.8	Storage locations – details showing site locations for backups that can be accessed in the event production data has been compromised.	A record of locations where data and backups are held must be documented and be compliant with GDPR requirements. Access to these locations must be available to teams during a production system outage. Access to these locations must be tested regularly to ensure availability of backups and data required for recovery.
5.2.9	Third-party dependencies – a register of third party suppliers required for the DRP must be fully documented.	It is essential that a register of the PSB third party supplies who will be required to successfully execute the DRP is maintained. The Public Service Bodies third party register must be available during the recovery process and must be reviewed regularly and where possible, tested regularly.
5.3	**Disaster Recovery Plan Practise (DRP)**	**Guidance Notes**
5.3.1	Utilisation of Disaster Recovery Plans to restore normal operation should be recorded and well-practised.	It is critical to the recovery process that the Disaster Recovery Plan (DRP) is tested regularly and findings from the test are fully documented. A lessons learned

		review should be undertaken and any learnings from the test and review must be incorporated into the update plan.
5.4	**Post-Incident**	**Guidance Notes**
5.4.1	Post-incident recovery activities shall inform the immediate future technical protection of the network, system or service, to ensure the issue cannot arise in the same manner again. Systemic vulnerabilities identified shall be remediated.	Vulnerabilities that lead to a cyber security incident must be identified, and remediation of vulnerabilities must be planned and executed. Where vulnerabilities cannot be mitigated, corresponding risks should be accepted and be raised with the PSB management team.
5.5	**Periodic Review**	**Guidance Notes**
5.5.1	All measures outlined in Section 5 should be subject to periodic review to consider changes in technology, practices and personnel.	Incident Response, Disaster Response and Communications should be reviewed regularly to ensure the effectiveness of the plans.
5.6	**Lessons Learned Process**	**5.6 Guidance Notes**
5.6.1	Public Service Bodies should use a lessons-learned process to gain value from incidents.	This process should review the effectiveness of the incident handling process and identify necessary improvements to existing security controls and practices. A culture of continuous improvement should be adopted to ensure that lessons learned are integrated in processes and procedures. Lessons learned meetings can also be held periodically for lesser incidents as time and resources permit. The information accumulated from all lessons learned meetings should be used to identify and correct systemic weaknesses and deficiencies in policies and procedures. Follow-up reports generated for each resolved incident can be important not only for evidentiary purposes but also for reference in handling future incidents and in training new team members.

Annex 1: NIST Framework Definitions

1. Identify Function

The Identify Function assists in developing an organisational understanding to managing cybersecurity risk to systems, people, assets, data, and capabilities. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organisation to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

Examples include:

- Identifying physical and software assets within the organisation to establish the basis of an Asset Management program.
- Identifying the Business Environment, the organisation supports including the organisation's role in the supply chain, and the organisations place in the critical infrastructure sector.
- Identifying cybersecurity policies established within the organisation to define the Governance program as well as identifying legal and regulatory requirements regarding the cybersecurity capabilities of the organisation.
- Identifying asset vulnerabilities, threats to internal and external organisational resources, and risk response activities as a basis for the organisations Risk Assessment.
- Identifying a Risk Management Strategy for the organisation including establishing risk tolerances.
- Identifying a Supply Chain Risk Management strategy including priorities, constraints, risk tolerances, and assumptions used to support risk decisions associated with managing supply chain risks.

2. Protect Function

The Protect function outlines appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event.

Examples of outcome Categories within this Function include:

- Protections for Identity Management and Access Control within the organisation including physical and remote access.
- Empowering staff within the organisation through Awareness and Training including role based and privileged user training.
- Establishing Data Security protection consistent with the organisation's risk strategy to protect the confidentiality, integrity, and availability of information.
- Implementing Information Protection Processes and Procedures to maintain and manage the protections of information systems and assets.
- Protecting organisational resources through Maintenance, including remote maintenance, activities.
- Managing Protective Technology to ensure the security and resilience of systems and assets are consistent with organisational policies, procedures, and agreements.

3. Detect Function

The Detect Function defines the appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events.

Examples of outcome Categories within this Function include:

- Ensuring Anomalies and Events are detected, and their potential impact is understood
- Implementing Security Continuous Monitoring capabilities to monitor cybersecurity events and verify the effectiveness of protective measures including network and physical activities
- Maintaining Detection Processes to provide awareness of anomalous events.

4. Respond Function

The Respond Function includes appropriate activities to act regarding a detected cyber security incident. The Respond Function supports the ability to contain the impact of a potential cyber security incident.

Examples of outcome Categories within this Function include:

- Ensuring Response Planning process are executed during and after an incident
- Managing Communications during and after an event with stakeholders, law enforcement, external stakeholders as appropriate
- Analysis is conducted to ensure effective response and support recovery activities including forensic analysis, and determining the impact of incidents
- Mitigation activities are performed to prevent expansion of an event and to resolve the incident
- The organisation implements Improvements by incorporating lessons learned from current and previous detection / response activities.

5. Recover Function

The Recover Function identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber security incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cyber security incident.

Examples of outcome Categories within this Function include:

- Ensuring the organisation implements Recovery Planning processes and procedures to restore systems and/or assets affected by cyber security incidents
- Implementing Improvements based on lessons learned and reviews of existing strategies
- Internal and external Communications are coordinated during and following the recovery from a cyber security incident

Annex 2: References

- CEN - CEN/CLC/JTC 13 (cencenelec.eu)

  Accessed 17/10/2022
- I.S. EN ISO/IEC 27000:2018
  Accessed 30/09/2022
- I.S. EN ISO/IEC 27001:2017
  Accessed 30/09/2022
- ISO/IEC 27005:2018

  Accessed 17/10/2022
- ISO/IEC 27002:2022

  Accessed 07/10/2022
- Centre for Internet Security (2021) CIS Benchmarks
  Accessed 07/10/2022
- ISACA (2021) CoBit - Control Objectives for Information and Related Technologies – An ISACA Framework
  Accessed 07/10/2022
- ISO - ISO/IEC 38500:2015 - Information technology — Governance of IT for the organization

  Accessed 17/10/2022
- NCSC (2018) 12 Steps to Cybersecurity – Guidance on Cyber Security for Irish Business
  Accessed 07/10/2022
- CISA (2021) Remote Access Guidelines
- Secure Password Policy pg. 5
- Join CiSP UK
- CIS Centre for Internet Security (2021) The 18 CIS Critical Security Controls
  Accessed 18/10/2021
- NIST (2005) CSRC SP 800-40 Rev 3. – Guide to Enterprise Patch Management Technologies
  Accessed 18/10/2021
- CISA - Trusted Internet Connections (TIC) 3.0 Remote User Use Case

Cyber Incident Response Plan Checklist V1

Template

Prepared by the Government Department of the Environment, Climate and Communications
National Cyber Security Baseline Standards Committee

Revision 1.0

Date:

Revision History

Revision Date	Items revised	Author	ICT Governance Committee Approved	Approved Management Board

1. Cyber Incident Response Plan (CIRP) Checklist

The National Cyber Security Baseline Standards Cyber Security Incident Response Plan (CIRP), is designed to enable all public sector bodies to develop their own CIRP in a manner = compatible with and complement existing Risk Management, Standards and Cyber Security Programs in use nationally and to be straightforward to apply. This checklist supports developing and reviewing your CIRP. It is set out under the CIRP headings, **Preparation**; **Detection and Analysis**, and **Containment**, **Eradication and Recovery** are structured round the = National Institute of Standards and Technology (NIST) framework Identify, Protect, Detect, Response, Recover (IPDDR).

This Cyber Incident Response Checklist assists in review of the Cyber Incident Response Plan from the template of the National Cyber Security Baseline Standards. Ireland's NCSC has guidance in place for Operators of Essential Services (OES) applies the NIST framework see Figure 1 below.

Figure 1: Ireland Network and Information Systems (NIS) Compliance Guidelines for Operators of Essential Services Framework Infographic

Source: DCCAE NIS Compliance Guidelines for Operators of Essential Services P22

2. Preparation: Identify, Protect

It is important to be as prepared as possible for a cyber-incident, is not just about preparing to handle an incident when it happens. It also entails the prevention of incidents by ensuring that systems, networks and applications are sufficiently secure.

Preparing to Handle Cyber Incidents	Location in CIRP Template **In Your CIRP?** Tick Box
Identify all essential contact information	
• Designate an incident response team First Responder within your organisation and second person for that post.	☐
• Designate all members of the cyber incident response team, names, contact details, title, role	☐
• Appoint a third-party incident response provider/ forensics team, document names, contact details, title, role	☐
• Contacts for external entities to be advised of cyber incident including NCSC, Regulatory Bodies, An Garda Síochána, others, contact details	☐
• All ICT staff contact details	☐
• Key Vendor contact list for all products/services contact details	☐
• Website Domain Names providers contact details	☐
Identify cyber incident management resources	
• Cyber Incident Response Team Operations Room Location	☐
• Alternate Room Location	☐
• Equipment, VC facilities, PCs, other listed	☐
• Catering arrangements, shift lengths etc.	☐
Serious cyber incidents Senior Executive Management Team (SEMT)	
• Protocol for Invoking the SEMT	☐
• Designate all members of the serious cyber incident SEMT team, names, contact details, title, role	☐
List of key assets and data and where they are located/hosted including Network diagrams.	☐

• Current baseline of IT systems' activities • Documentation of IT systems and software versions • Back-ups	☐ ☐
Develop the relevant plans including: • CIRP – hard copy 3 locations one off main site • CIRP – electronic copy • CIRP communications plan • Business continuity plans • Disaster recovery plans	☐ ☐ ☐ ☐ ☐
Develop templates for documenting, reporting including: • Situation Update • Incident Log • Resolution Action Plan • Evidence Register • Lessons Learned Report	☐ ☐ ☐ ☐ ☐
Identify and understand the type of attacks that could affect your organisation. Over time develop scenarios and action plans to deal with each type of attack under Network Attack, Employee Attack, Physical Security and use for Awareness Training. • Computer Crime examples • Computer Enabled Crime examples • Malware examples • Phishing, Vishing examples • Distributed denial of service examples • Ransomware examples • Data breach examples • Data corruption examples • Physical security examples e.g. cyber hacker defaults access doors to shut. **Useful resources include:** NCSC, ENISA, NIST, EUROPOL, An Garda Síochana	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐

3. Detection and Analysis: Detect, Respond

There is no single process for detecting a Cyber incident, there are many routes including, monitors, sensors, unusual network activity, anti-virus alerts, NCSC alerts, staff call the ICT helpdesk, a member of the public reports a security vulnerability, advised of a threat to the organisation.

Detecting and Analysing Cyber Incidents	**Location in CIRP Template** **In Your CIRP?** Tick Box
Detect: Monitor Security software (e.g., Intrusion Detection Systems [IDS], Security Information and Events Management System [SIEM], anti-virus software, third-party monitoring services etc.).	
• Monitor Logs (e.g. operating system logs, service and application logs, network device logs, netflow logs etc)	☐
• Monitor Publicly available information (e.g. NCSC alerts, alerts from products/services vendors on vulnerabilities, etc)	☐
• Monitor people within your organisation in accordance with your HR/Information Security Policy	☐
• Other Analytics Review	☐
Monitoring for potential Cyber Weaknesses. Check often and be prepared for cyber incidents that use common attack vectors, such as:	
• Misconfigured systems	☐
• Internet downloads	☐
• Poor cyber hygiene practices (e.g. use of weak or default passwords, use of outdated software, etc)	☐
• Human lapses	☐
• Poor patch management	☐
• Poorly designed web applications	☐
• Authorised third parties	☐
Analyse from ongoing monitoring or Cyber Incident reported	
• Have you notified First Responder that an initial assessment is being made	☐

• Have you correlated events against the baseline to determine if an incident has occurred • Have you checked incidents against known threats precursors and indicators • Have you made an initial assessment of the scope and nature of the incident, particularly whether it is a malicious act or a technological glitch • Have you confirmed whether an incident has occurred or is continuing to occur? • Have you prioritised the incident handling activities, including whether to activate crisis management, and crisis communications plans • Have you informed the First Responder • First Responder convenes Cyber Incident Response Team meeting	☐ ☐ ☐ ☐ ☐ ☐ ☐
Cyber Incident Response Team meeting analysis determines a response strategy and document the following: • What type of incident is this? Example: virus, worm, intrusion. • Is the incident still in progress? • What system or systems are being targeted, where are they located physically and on the network? • What data or property is threatened how critical is it? Document this • If personal data is threatened, what are the risks to the data subjects affected? • What is the impact on the business should the attack succeed? Is it minimal, serious, or critical? • Is the response urgent? • Can the incident be quickly contained? • Will the response alert the attacker? • Is SEMT to be notified/invoked • Evidence Gathering Procedures in place • Containment and Evidence Gathering processes invoke	 ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐

4. Containment, Eradication, Recovery: Respond, Recover

This is a critical stage of cyber incident response and recovery. The actions flow from plans to respond to detection of a cyber-incident and analysis information and indicators of compromise.

Contain, Eradicate and Recovery from Cyber Incidents	**Location in CIRP Template** **In Your CIRP?** Tick Box
Containment includes:	
• Deploy additional monitoring tools to identify the malware behaviour:	☐
• Isolate all or parts of the compromised network by disconnecting all affected systems	☐
• Re-route or filter network traffic	☐
• Firewall filtering	☐
• Close vulnerable ports and mail servers	☐
• Block further unauthorised access to the system	☐
• Helpdesk updates answer machine to inform about major incident inform users to stop all activity on their devices until told otherwise	☐
Eradication includes:	
• Isolate all activity on the networks to restrict further incidents.	☐
• Wiping out the malware	☐
• Disabling breached user accounts	☐
• Patching vulnerabilities exploited. This should be applied to all affected hosts within the organisation	☐
Evidence Preservation including: This will be for (1) incident resolution, (2) possible legal action.	
• Summary of the incident	☐
• Incident indicators	☐
• System events	☐
• Actions taken during the incident	☐
• Logs of affected systems	☐
• Forensic copies of affected systems	☐
• Hard drive images and raw images	☐

• RAM images • IP addresses • Network packet captures and flows • Network diagrams • Log and configuration files • Databases • IR/investigation notes • Screenshots • Social media posts • CCTV, video and audio recordings • Documents detailing the monetary cost of remediation or loss of business activity • Taking and gathering statements. • Asset handover processes (if required)	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐
Disaster Recovery and Back-ups. This may entail: • Restoring systems from backups Re-install the affected system(s) from scratch and restore data from backups. Preserve evidence before doing this. • Make administrators and users change passwords. • Be sure the system has been hardened by turning off or uninstalling unused services. • Patch system. • Be sure real time virus protection and intrusion detection is running. • Be sure the system is logging the correct events and to the proper level • Rebuilding systems from scratch • Tightening network perimeter security • Confirming the integrity of business systems and controls • Continue to the network for any anomalous activity or signs of intrusion	 ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐
Knowing your Stakeholders and/or Fiduciary Obligations Notify stakeholders and affected parties in line you're your Communications Plan. • SEMT	☐ ☐

• Management Board/Board of Directors • Regulators, law enforcement and other government agencies • 3rd party Vendors • Stakeholders • Media	☐ ☐ ☐ ☐
Standing Down • First Responder/SEMT stands down cyber incident response team • Incident Response Team report prepared • Forensic Team report prepared	☐ ☐ ☐

5. Post-Incident Activity: Identify, Protect

A full review of the cyber incident including response, recovery and future steps ensures risk mitigation for this particular incident.

Post-Cyber Incident Activity	Location in CIRP Template **In Your CIRP?** Tick Box
Identify and resolve deficiencies in systems and processes that led to the incident	
• Identify and resolve deficiencies in planning and execution of your incident response plan.	☐
• Assess if additional security measures are needed to strengthen the security posture of your organisation.	☐
• Assess if governance factors were involved and what additional governance steps may be needed	☐
• Assess what additional actions may need to be undertaken and implement.	☐
• Depending on the incident, organisations may need to consider higher levels of system logging or network monitoring.	☐
Lessons learned report	
• Lessons Learned Report completed	☐
• Agreed with Incident Management Team, SEMT	☐
• Communicated to stakeholders as appropriate, in accordance with communications plan.	☐
• Accompanying action plans developed to respond to common incidents should be accessible and any updates communicated to relevant parties (e.g. employees, etc.).	☐
• Communications with the employees and key stakeholders	☐
• User awareness and training updated	☐
Ongoing post lessons learned report	
• Update the CIRP	☐
• Ongoing criminal reports/processes (if needed)	☐
• Regular reviews and updates of CIRP plans at regular scheduled intervals)	☐
• Walk-through/exercise the plans	☐

6. References

- Government of Singapore, Cyber Security Awareness Alliance (2021) Incident Response Checklist. Accessed 07 October 2022.
- The United States Department of Commerce, The United States National Institute of Standards and Technology (April 2018), Framework for Improving Critical Infrastructure Cybersecurity.
- The United States Department of Commerce, National Institute of Standards and Technology (August 2012), NIST Special Publication 800-61 Rev2. Computer Security Incident Handling Guide.
- The United States Department of Justice (September 2018), v2.0. Best Practices for Victim Response and Reporting of Cyber Incidents.
- Government of Ireland, Department of Communications, Climate Action and Environment (2019) NIS Compliance Guidelines for Operators of Essential Services (OES)

7. Useful Resources

The National Cyber Security Centre (NCSC)

Link: https://www.ncsc.gov.ie

Cyber Security Baseline Standards Queries

Link: publicsectorcybersecurity@decc.gov.ie

How to Report a Public Security Incident

Link: info@ncsc.gov.ie

As a member of the public if you feel that you have experienced a cyber security incident that may have a national impact please contact the NCSC.

How to Report a Governmental Security Incident

Link: certreport@decc.gov.ie

If you believe that you are experiencing a cyber security incident that is of national concern and wish to notify us directly you may email us at info@ncsc.gov.ie.

If you wish to report a security incident and you are an agent of one of NCSC's constituents (e.g., an official in a government department with the authority to make such a report) please email incident@ncsc.gov.ie or certreport@decc.gov.ie.

Irish National Cyber Security Centre Resource Page

Link: https://www.ncsc.gov.ie/guidance/

- Quick Guide: Cyber Security for Schools
  This quick guide will highlight the cyber risks posed to schools and the key priority measures to consider mitigating against these risks.
- Quick Guide: Ransomware How to #BreakTheChain
  Ransomware operators are not only interested in critical infrastructure, ransomware attacks can affect all types of organisations, both large and small. This quick guide is for organisations to understand the steps in a Ransomware Attack Chain, and more importantly how good cybersecurity practices will allow you to stop an attacker and #BreakTheChain.

- NCSC Cyber Security for Political Parties and Candidates
  Detailed guidance for political parties and politicians in relation to cybersecurity. This guidance covers the following:
    - An outline of the potential cybersecurity risks for political candidates or political parties
    - Advice for all political candidates for election so that they might better protect themselves and their data
    - Guidance for management and IT administrators in political parties
    - Services that the NCSC and others will be able to offer to candidates in securing their data.
- Quick Guide: Cyber Security Best Practice for Electoral Candidates
  This cyber security best practice quick guide has been produced by the NCSC to assist electoral candidates in implementing key priority preventive measures that can help to reduce the likelihood of them becoming a victim of a cyber-attack and the negative impacts that may result.
- Working from Home Security Advice
  With remote working becoming part of our day to day life, it is important that you ensure your home office matches the level of security you would expect to find in your professional office environment. This detailed guidance document covers some important steps you can take to achieve this.
- 12 Steps to Cyber Security for Businesses
  This detailed guidance is intended to be used by businesses as a suggested activity plan which may be undertaken on a month-by-month basis over a suggested 12 month period to improve cyber resilience.

ENISA the European Union Agency for Cybersecurity Resources

- CSIRT Services — ENISA (europa.eu)
  These pages contain information about ENISA's work on cooperation between CSIRTS and other operational communities.
- CSIRTs and communities — ENISA (europa.eu)
- Cyber Crisis Management — ENISA (europa.eu)

- Cybersecurity Education — ENISA (europa.eu)
  The European Union Agency for Cybersecurity, ENISA has placed Capacity Building as a strategic objective on its new strategy. In this content ENISA is committed to support and strengthen the enhancement of cybersecurity skills and competence across at all levels, from the non-experts to the highly skilled professionals.
- Data Protection — ENISA (europa.eu)
  The General Data Protection Regulation (GDPR), aims at addressing these risks by reinforcing individuals' rights in the digital era and enabling them to better control their personal data online. At the same time modernised and unified rules will allow businesses to make the most of the opportunities of the Digital Single Market (DSM) also benefiting from increased consumer trust.
- National Cybersecurity Strategies — ENISA (europa.eu)
  In a constantly changing cyber threats environment, EU Member States need to have flexible and dynamic cybersecurity strategies to meet new, global threats. A national cybersecurity strategy (NCSS) is a plan of actions designed to improve the security and resilience of national infrastructures and services.
- Standards and Certification — ENISA (europa.eu)
  Since its creation, ENISA has been active in the field of standardisation by cooperating with European and international Standards Developing Organisations (ESOs and SDOs), being ETSI, CEN, CENELEC, and stakeholders' communities alike in the area of NIS standardisation.
- Threat and Risk Management — ENISA (europa.eu)
  Risk and threat assessment are the pillars of security risk management and as such, vital methods towards cyber-protection and cyber-risk mitigation

CISA (US Cybersecurity & Infrastructure Security Agency) – Cybersecurity Resources

Link: https://www.cisa.gov/cisa-cybersecurity-resources

To decrease cybersecurity risks and protect yourself online, CISA offers the following resources to share in your communities and with your stakeholders. These tools are not only valuable during Cybersecurity Awareness Month but throughout the year.

Telework Guidance and Best Practices

Link: CISA's Telework Resources

CISA brings our industry partners and the federal government together to improve American cyber and infrastructure security. CISA offers these resources to assist organisations and teleworkers in being secure when working remotely.

Assessments, Prevention, and Response Resources

Link: CISA's Cybersecurity Hub

CISA offers a wide range of cybersecurity assessments that evaluate operational resilience, cybersecurity practices, organisational management of external dependencies, and other key elements of a robust cybersecurity framework. CISA's cybersecurity assessment services are available upon request and offered strictly on a voluntary basis.

Cybersecurity Awareness and Best Practices Resources

Link: CISA's Cyber Essentials

CISA's Cyber Essentials is a guide for small business leaders and local government agencies to develop an actionable understanding of how to implement organisational cybersecurity best practices. For more information, check out the Cyber Essentials Toolkits, a set of modules that breaks down the CISA Cyber Essentials into bite-sized actions for IT and C-suite leadership to work toward full implementation of each Cyber Essential.

Misinformation, Disinformation, and Malinformation Resources

Link: Mis, Dis, Malinformation (MDM)

CISA's MDM Team is charged with building national resilience to mis-, dis-, and malinformation (MDM) and foreign influence activities. The MDM Team does this by helping the American people and DHS stakeholders understand the scope and scale of MDM activities targeting elections and critical infrastructure, and by enabling them to take actions to mitigate risks associated with MDM.

Mitigating Cyber Risks to The Nation's Critical Infrastructure

Link: National Risk Management

In today's digitizing world, organisations are increasingly integrating cyber systems into their

critical infrastructure operations. Whether it be protecting 5G wireless technology, our nation's pipeline infrastructure, or the ICT supply chain, CISA identifies threats and vulnerabilities to these assets, systems, and networks that provide functions necessary for our way of life.

- Enisa is the European Union Agency for Cybersecurity
- More information on the NIST Cyber Security Framework can be found at Cybersecurity Framework | NIST
- US Cyber Security Infrastructure Security Agency Homepage | CISA
- CISA Cyber Essentials
- UK National Cyber Security Centre
- SANS Institute - cooperative for information security thought leadership
- Best Practices for Victim Response and Reporting of Cyber Incidents

Please note: all reports to the ncsc.gov.ie are treated in the strictest confidence.

Staying Up to Date

Link: https://nvd.nist.gov.

It is critical that you stay up to date on security issues with the infrastructure and software in use in your organisation. Most vendors of software and hardware have an email service to subscribe to security alerts on their websites.

The NVD is the U.S. government repository of standards-based vulnerability management data and can be found here. The site provides updates on new discovered vulnerabilities.

MITRE ATT&CK®

MITRE ATT&CK is beneficial for organisation who want to understand how to defend organisations. MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

RSS Resources

RSS is one just one way of staying up to date with what is going on in the work of Cyber Security and Information Security.

RSS (Wikipedia) (RDF **Site Summary** or **Really Simple Syndication**)[2] is a web feed[3] that allows users and applications to access updates to websites in a standardized, computer-readable format. Subscribing to RSS feeds can allow a user to keep track of many different websites in a single news aggregator, which constantly monitor sites for new content, removing the need for the user to manually check them. News aggregators (or "RSS readers") can be built into a browser, installed on a desktop computer, or installed on a mobile device.

- **Krebs on Security** https://krebsonsecurity.com/feed/
- **Dark Reading** https://www.darkreading.com/rss/all.xml
- **Schnier on Security** https://www.schneier.com/blog/atom.xml
- **Bleeping Computer** https://www.bleepingcomputer.com/feed
- **The Hacker News** http://feeds.feedburner.com/TheHackersNews?format=xml
- **Threatpost** https://threatpost.com/feed/
- **NIST Insights** https://www.nist.gov/blogs/cybersecurity-insights/rss.xml
- **Helpnet Security** https://www.helpnetsecurity.com/feed/
- **CISA Alerts** https://www.us-cert.gov/ncas/alerts.xml

8. Revisions to this document

Section	Revision	Text
1.6.2	Moved	Section moved to 1.6.3
1.6.2	Insert	Inserted section on third-party register. "*Third-party dependencies – a register of third-party suppliers must be developed and maintained by Public Service Bodies.*"
2.12.1	Edit	"Multi-Factor Authentication". Clause edited to be clearer around MFA.
2.12.2	Removed	Text removed and encapsulated into 2.12.1
2.12.3	Edit	Renumbering change
4.6	Edit	Traffic Light Protocol Updated to version 2.0 which is the current version of TLP standardized by FIRST. It is authoritative from August 2022 onwards
Annex 2 CIRP	Edit	CIRP references to additional Appendix removed to improve document
Annex 3	Edit	Updated to include CEN/CLC/JTC 1 - Cybersecurity and Data Protection and latest ISO 27000,27001,27005 and 27002 references