

***GUIDANCE – DELETE TEXT
BOX UPON COMPLETION***

Insert your organisation logo here
and in the header of the document.

<ORGANISATION>

<IT Security Team>

Cyber Incident Response Plan

Version: v1.1

Date: 18 Aug 2019

Owner: <ORGANISATION>

VERSION CONTROL

Version No	Updated By	Reason for Update/Area Updated	Date Updated
1.0	NCC Group	Tailored CIRP for cyber incident readiness project delivery	26 th July 2019
1.1	SG CRU	Amendments after proof Reading and consultation with stakeholders	18 th Aug 2019

APPROVAL RECORD

Version No	Approval Body	Approval Date	Effective Date	Review Date
1.1	<INSERT LOCAL OWNER>			

DISTRIBUTION LIST

Name	Position
	IT Security Manager
	Head of Cyber and Defence
All members of the Cyber Incident Response Team	
All members of the Crisis Management Team	
All heads of Business Units	



- 1. Introduction to the Cyber Incident Response Plan (CIRP)..... 4**
 - 1.1 Purpose..... 4
 - 1.2 Central Notification and Co-ordination Policy..... 6
 - 1.3 Alignment to UK National Cyber incident Reporting Protocols..... 6
 - 1.4 Scope..... 7
- 2. Management Roles and Responsibilities..... 8**
 - 2.1 Cyber Incident Response Team (CIRT) & Crisis Management Team 8
 - 2.2 RACI Matrix 9
 - 2.3 Updates to the CIRP..... 11
- 3. Communications..... 12**
 - 3.1 Management Notification 12
 - 3.2 Human Resources (HR) Notification 12
 - 3.3 Legal Services Notification 13
 - 3.4 Third Parties Notification..... 13
- 4. Cyber Incident Response Process 14**
 - 4.1 Step 1 – Prepare..... 15
 - 4.1.1 Required documentation 15
 - 4.1.2 Preparation 16
 - 4.1.3 Pre-requisites..... 16
 - 4.1.4 Training & Awareness 16
 - 4.1.5 Testing 17
 - 4.2 Step 2 & 3 – Identify and Report 18
 - 4.2.1 Incident Types 19
 - 4.2.2 Data Classification 20
 - 4.2.3 Reporting to the ICO..... 21
 - 4.3 Step 4 – Analyse and Investigate 23
 - 4.3.1 Cyber Incident Severity Assessment..... 23
 - 4.4 Step 5 – Containment..... 29
 - 4.5 Step 6 – Eradicate 31
 - 4.6 Step 7 – Recovery 32
 - 4.7 Step 8 & 9 – Reporting and Lessons Identified 33
- 5. Appendix A – Forensic Imaging Guide..... 35**
- 6. Appendix B – Cyber Incident Response Team (CIRT) Contact Information..... 36**
- 7. Appendix C – Crisis Management Team (CMT) Contact Information..... 37**
- 8. Appendix D – Third Party Support Services Contact Information..... 38**
- 9. Appendix E – Scottish Public Sector Cyber Incident Central Notification and Coordination Policy
39**
- 10. Appendix F – Notifiable Reporting Form..... 40**
- 11. Appendix G – NCSC Incident Categorisation Framework..... 44**
- 12. Appendix H – List of Abbreviations 46**

1. Introduction to the Cyber Incident Response Plan (CIRP)

GUIDANCE – DELETE TEXT BOX UPON COMPLETION

Document implementation guidance

This document has been designed so that a Scottish Public Sector organisation can create a bespoke Cyber Incident Response Plan CIRP based on recognised good practice. The sections are designed to be tailored to best suit the organisation but provide suggested content for consideration.

GREEN highlighted sections will simply require insertion of the Organisation or name of responsible person/team.

Sections with a red text box contain further guidance on the section to be tailored. The author should **DELETE** the red box upon completion of the section.

Sections marked as **MANDATORY SECTION** are considered as **Core Components** and should remain to ensure consistency across the Scottish Public Sector. Where organisations outsource responsibility for certain activities or indeed complete sections then this must be interpreted within the CIRP to ensure it is clear where the responsibility lies for undertaking the tasks contained therein.

1.1 Purpose

Scottish Government's Cyber Resilience: Public Sector Action Plan¹ encourages all Public Sector organisations to put in place appropriate cyber incident response plans as part of wider response arrangements, and ensure these are aligned with Scottish Public Sector Cyber Incident Central Notification and Co-ordination policy.

The purpose of this plan is to provide operational structure, processes and procedures to **<ORGANISATION>** personnel, so that they can effectively respond to incidents that may impact the function and security of digital assets, information resources, and business operations.

Cyber-attacks can quickly escalate and become a significant business disruptor requiring both business continuity and consequence management considerations. Whilst much of the CIRP will be managed within the IT Security environment, early consideration should be given to engaging both Business Continuity and Resilience Leads in order that the wider issues can be managed. Business Continuity and Resilience leads in the organisation must therefore be familiar with the CIRP.

The CIRP will assist the **<ORGANISATION>** in identifying, managing, investigating, and remediating various types of cyber incidents. It describes the processes for initiating a response and establishing the structure needed to ensure response execution. This CIRP will also reference procedural documentation that provides operational-level details specific to handling the various incident types.

The CIRP cannot anticipate and provide guidance for all potential incidents. Management and incident responders should consider the current situation, business impact, and security needs of the **<ORGANISATION>** and balance those against the guidance and recommendations provided by the CIRP.

This plan is based on a number of recommended industry best practices including:

¹ Available at: <https://www.gov.scot/publications/cyber-resilience-strategy-scotland-public-sector-action-plan-2017-18/> (last visited 24th April 2019)

- The Standard of Good Practice for Information Security 2018²
- Existing cyber incident response documentation provided by Scottish Public Sector organisations
- ISO/IEC 27035: 2016 Information Security Incident Management³
- NCC Group experience and knowledge

² Available at: <https://www.securityforum.org/tool/the-isf-standard-good-practice-information-security-2018/> (last visited 24th April 2019)

³ Available at: <https://www.iso.org/standard/60803.html> (last visited 24th April 2019)

1.2 Central Notification and Co-ordination Policy

***GUIDANCE – DELETE TEXT BOX UPON COMPLETION* - MANDATORY SECTION**

Section 1.2 and 1.3 recognise the requirement to escalate a cyber incident in accordance with the Scottish Public Sector Cyber Incident Central Notification and Co-ordination Policy. These sections are critical to align with Scottish Government's ambition and requirements to improve incident response across the public and private sectors.

All Scottish Public Sector organisations should comply with the Scottish Public Sector Cyber Incident Central Notification and Co-ordination Policy (Appendix [E](#) and [F](#)) which outlines the policy and procedures for notifiable cyber incidents impacting on Scotland's public services.

The trigger for consideration of such notification is defined as incidents or attacks against Scottish public sector network information systems which will:

- Have the potential to disrupt the continued operation of the organisation or delivery of public services; and/or
- Carry a likelihood that other public, private or third sector organisations may experience a similar attack, or that the incident could spread to those organisations; and/or
- Could have a negative impact on the reputation of the Scottish public sector or Scottish Government; and/ or
- Carry the likelihood of Scottish Parliament or national media interest.

In such circumstances there is a requirement to notify the National Cyber Security Centre (NCSC), Scottish Government Cyber Resilience Unit (SG CRU) and Scottish Government Resilience officials for incident management and co-ordination purposes and also Police Scotland for crime investigation considerations. This reporting mechanism is intended to enable the appropriate levels of external support to be considered that might not be immediately obvious to organisational IT security teams who are focussed on dealing with the incident at hand.

1.3 Alignment to UK National Cyber incident Reporting Protocols

The CIRP acknowledges the National Cyber Incident Management Policy (NCIMP – this is a restricted circulation policy) and the Scottish Public Sector Cyber Incident Central Notification and Co-ordination Policy, that set out the process for managing cyber incidents that have a national impact in both Scotland and the UK context. The NCIMP aligns with the Central Government Arrangements for Responding to an Emergency: Concept of Operations (CONOPS). The NCSC is responsible for officially 'declaring' a cyber incident that requires management and co-ordination at a UK level. For context and information on the NCSC incident categorisation framework⁴ please see Appendix [G](#).

⁴ Available at <https://www.ncsc.gov.uk/news/new-cyber-attack-categorisation-system-improve-uk-response-incidents> (last visited 25th April 2019)

1.4 Scope

An **Information Security Incident** is an incident that specifically impacts upon <ORGANISATION> information. E.g.: the loss, theft, damage or destruction of information; or an item of IT equipment on which such information is stored. Information Security Incidents typically involve a potential impact to the confidentiality or integrity of <ORGANISATION> information. Events affecting the availability of <ORGANISATION> information are typically handled as IT Service Incidents by IT Service Management processes in the first instance; as such processes are focused on restoring service availability to users as quickly as possible. Loss of service availability is likely to become a security issue where it stems from a deliberate hostile act, or where change is required to avoid repetition.

A **cyber incident** is the subset of Information Security Incidents that affects digital data or IT assets, and does not involve any hardcopy information. For example: a user account compromise, a network intrusion or a malware outbreak.

Cyber incident Management is the process of handling all cyber incidents in a structured and controlled way. This plan ensures that:

- All cyber incidents are managed quickly and efficiently
- A consistent approach is implemented to manage cyber incidents
- The damage caused by a cyber incident is minimised
- The likelihood of recurrence of the security incident is reduced by the review and implementation of appropriate measures

The scope of this plan is limited to cyber incidents affecting the IT services, electronic data and associated digital assets within the control of <ORGANISATION>. For the purpose of this plan, the following list of IT incidents have not been treated as cyber incidents and therefore are outside the scope of this document:

- Software problems and technical failures not caused by malicious activity
- Unavailability of the corporate IT network and / or systems
- Performance problems with the corporate IT network and / or systems
- Hardware problems and failures

2. Management Roles and Responsibilities

2.1 Cyber Incident Response Team (CIRT) & Crisis Management Team

***GUIDANCE – DELETE TEXT BOX UPON COMPLETION* - MANDATORY SECTION**

CIRTs can vary based on the type and culture of an organisation, below are a number of suggested roles, personnel and various departments that can form the CIRT. The CIRT should include a team of personnel who have sufficient skills and experience to manage the differing aspects of cyber incidents. It is important that some members of the CIRT have the authority to make business decisions and escalate incidents to the appropriate team/stakeholders. The CIRT should also consider internal and external stakeholders such as the legal department, finance, human resources (HR), third parties and media. Below you should list the key personnel and departments that form the CIRT for your organisations.

A Core Incident Response Team is a smaller team which comprises of the IT staff who will have routine responsibility for identifying, assessing and triaging all IT security incidents. Incidents will often be escalated to the CIRT via the lead for the team.

Cyber incidents are managed (triage, containment, eradication, lessons identified and reporting) by the CIRT. This team is responsible for analysing security breaches and taking any necessary responsive measures and advising Senior Management / Board of key breaches and the response developed. In most instances the CIRT will be informed of and brought together as a team when relevant breaches/risks have been raised to the group after an assessment of risk has been made by the <HEAD OF IT OPERATIONS>. It may be that a smaller team from within IT security (Core IT CIRT) will assess and classify the incident prior to escalation to the CIRT which will likely involve wider non IT personnel. References to an Extended CIRT will relate to external parties brought in as and when required to support the CIRT.

A Crisis Management Team (Senior Management Team) may be formed to deal with the Strategic consequences and decisions that arise from the CIRT incident management. Within <ORGANISATION>. This team will consist of <INSERT AS RELEVANT>.

The Core IT CIRT includes key operational personnel necessary to identify and triage all cyber incidents within <ORGANISATION>. This team will be headed by the <Information Security Officer> supported by the following personnel.

- Security Architect
- Security Analyst
- Network Operator
- Systems Administrator
- Service Desk Support
- <Others>

The CIRT includes key personnel from the following departments:

- Chief Information Security Officer (CISO) – Incident Owner

- Head of Operations or IT Senior Officer (ITSO) – Incident Manager
- Information Security Officer (ISO)
- Senior Information Risk Owner (SIRO)
- Core Incident Response Team Lead (IT Incident Response Team Lead)
- Human Resources (HR)
- Legal Services Rep
- Finance Rep
- Audit Rep
- Physical Security Rep
- Communications Lead
- Policy Area Lead
- Resilience Lead
- Business Continuity Lead
- Data Protection Officer (DPO)
- Other relevant employees, contractors and third parties

The CIRT may be extended (Extended CIRT) to incorporate external partners and agencies where this is deemed appropriate in circumstances to add value to the management of the incident. This will often be the case in more complex incidents that lead to escalation. This may for example include;

- Scottish Government
- Police Scotland
- NCSC
- 3rd party security specialists
- Regional Resilience Co-ordinator
- External legal services

2.2 RACI Matrix

Delegation, clarity and accountability are crucial in dealing with cyber incidents that have escalated to requiring a CIRT to be formed. The **RACI matrix** is a useful tool that assigns responsibility and maps out tasks, milestones or key decisions involved in completing a project such as managing an incident. It assigns which roles are Responsible for each action item, which personnel are Accountable, and, where appropriate, who needs to be Consulted or Informed. It is a very useful tool in the context of developing a CIRP.

Responsible: Refers to those who do the work to complete the task. Who's doing the work?

Accountable: Designates the person who ultimately answer for the results of an activity, and also who delegates the work to the people who will execute it. Who is making the decisions?

Consulted: Refers to those who should be heard on the related activity, and with whom there is two-way communication. Who will be communicated with regarding incident decisions and tasks?

Informed: Designates those who sought to be kept up-to-date on the progress of the activity, and with whom there is just one-way communication. Who will be updated on decisions and actions during the incident?

Figure 1 outlines where key responsibilities in the incident handling process fall in the form of a Responsible / Accountable / Consulted / Informed (RACI) matrix. <ORGANISATION TAILORED SECTION>

***GUIDANCE – DELETE TEXT BOX UPON COMPLETION* - MANDATORY SECTION**

RACI is a form of responsibility assignment presentation, and is named after the four most common responsibilities used: Responsible, Accountable, Consulted, and Informed.

When completing the RACI matrix, the roles should be tailored to your organisation

Task No.	Task	IT Managed Service Providers	Management Board	<ORGANISATION> ISM	Managed Service Provider	CIRT	Other <ORGANISATION> Personnel	Third Party Stakeholders	Impacted Individuals	Law Enforcement and Regulators	Insurers
1	Identifying Incidents	R	-	A,R	R	-	R	R	-	-	
2	Reporting Incidents	R	-	A, R	R	-	R	R	-	-	
3	Capturing Incidents	-	-	A	R	-	-	-	-	-	
4	Assigning Incidents	-	-	A	R	-	-	-	-	-	
5	Investigation of Incidents	R	I	A	R	C	R	R,(I)	(I)	(I)	(I)
6	Containment of Incidents	R	I	A	R	C	R	R	(I)	(I)	(I)
7	Eradication of Incidents	R	I	A	R	C	R	R	-	(I)	(I)
8	Recovery from Incidents	R	I	A	R	R,C	R	R	(I)	(I)	(I)
9	Review & Learn from Incidents	R,C	I	A,R	R	R,C	C	C	-	(I)	(I)
10	Improve / Prevent Recurrence of Incidents	R,C	I	A,R	R	C	R	R	(I)	(I)	(I)
11	Policy Impact	-	I	I		R,C				(I)	
12	Resilience and Business Continuity Assessment	-	I	I		R,C				(I)	

Figure 1 – <ORGANISATION> RACI Matrix

Governance of cyber incident policies, procedures and planning, is the responsibility of the **<ORGANISATION RESPONSIBLE TEAM – OFTEN THE IT SECURITY TEAM>** which includes:

- CISO
- Head of Operations
- Security Operations Centre
- Service Desk
- Network Operations and Infrastructure
- Systems Administrator and Web Services

Consideration should be given to inclusion of Resilience and Business Continuity leads for escalation and co-ordination planning and Communications leads for media and reputational management.

2.3 Updates to the CIRP

***GUIDANCE – DELETE TEXT BOX UPON COMPLETION* - MANDATORY SECTION**

CIRPs are living documents. Ownership and updates to the CIRP are critical to ensure the plan remains relevant, contacts are up to date and lessons identified are fed back into the plan. Assignment of ownership should be established from the early stages of the CIRP development. This responsibility should sit with the owner of the CIRP; this is typically the CISO or Information Security Manager of an organisation.

Ownership of the plan rests with the **<ORGANISATION RESPONSIBLE PERSON>** and will be reviewed on a **<BI MONTHLY>** and/or after an incident has occurred. Ensuring ownership and updates to contact details is critical to the on-going operations of the CIRP.

3. Communications

***GUIDANCE – DELETE TEXT BOX UPON COMPLETION* - MANDATORY SECTION**

Below are recommended escalation processes to consider. This should be tailored to your existing communications processes.

RESILIENT COMMUNICATIONS - The ability to contact key members of staff within the Core IT CIRT, CIRT and the Crisis Management Team is critical in the effective handling of a cyber-attack. As corporate communications both email and phone may be impacted and unavailable alternative methods to contact key staff should exist.

3.1 Management Notification

The CIRT or Core IR CIRT will keep the relevant management and associated third parties informed of the details of all confirmed **CRITICAL** or **HIGH** severity cyber incidents via the appointed Single Point of Contacts (SPoCs). Identified management and third parties include the following:

- The relevant Business Unit Managers, Policy Leads and Corporate Comms should be notified of the incident and kept up to date with progress to allow them to manage their customers/staff and other stakeholders.
- Security Management Notification - Where there is a confirmed critical security related incident, the **<ORGANISATION RESPONSIBLE PERSON – CISO/CRO>** must be notified and kept up to date with progress.
- Senior Information Risk Owner (SIRO)
- Communication with regulatory authorities as required.
- Contact contracted security specialist third parties for assistance as required.
- Core respondents within the Scottish Public Sector Cyber Incident Central Notification & Co-ordination Policy
- Resilience Partnership for early multi agency support and co-ordination arrangements.

3.2 Human Resources (HR) Notification

The CIRT or Core IT CIRT will notify HR of all confirmed cyber incidents where a significant breach of information security policies concerning a current or former member of staff. HR will be responsible for taking actions including:

- Ensuring cyber security training in place for staff
- If required taking disciplinary actions
- If required, cooperating with the police and other legal bodies
- Managing the corporate response to press, social media, PR
- Co-ordinating with legal services where current or former members of staff are in breach of contract

3.3 Legal Services Notification

The CIRT or Core IT CIRT will notify all confirmed cyber incidents where theft or other malicious actions could result in a prosecution to Legal services. Legal services will be responsible for taking actions including:

- Informing and cooperating with the police and other external legal entities

3.4 Third Parties Notification

The CIRT or Core IT CIRT will notify relevant third parties all confirmed **CRITICAL** or **HIGH** severity cyber incidents where the incident has compromised their information, such as payment card/ account data. This would also include situations where the third party has lost data or the data has been compromised that relates to **<ORGANISATION>** and/or our customers. Incidents that would need to be notified include:

- Loss of Personally Identifiable Information (PII), such as personal details including name, address and telephone numbers of staff or customers **<REPORTING TO THE ICO>**
- Key logger or card skimmer device found
- DDoS attack where DNS need to be modified
- Contacting software vendors for modifications to applications to remove exploited vulnerabilities

The CIRT or Core IT CIRT will notify Cyber incidents requiring support from trusted third party service providers such as ISP, DNS management, Application Development and Penetration Testing where there is a need to consult with them with regards supporting the management of the incident.

The CIRT or Core IT CIRT will notify Cyber incidents that meet the requirements of the Scottish Public Sector Cyber Incident Central Notification and Co-ordination Policy to;

- Police Scotland Cyber Unit
- The National Cyber Security Centre
- The Scottish Government Cyber Resilience Unit
- The Scottish Government Resilience Room (SGoRR)
- Scottish Government Policy Area Lead (where relevant)
- **OTHER CENTRAL CO-ORDINATING BODY AS RELEVANT**

Where incidents do not meet the thresholds of the above policy the CIRT or Core IT CIRT will still consider notifying Cyber incidents to the NCSC and / Police Scotland and Scottish Government CRU where there is value in improving the rich intelligence picture, other public sector bodies could take mitigation steps or there is a crime worthy of investigation.

4. Cyber Incident Response Process

Figure 2 sets out the end-to-end incident handling process in overview. The relationship between **<ORGANISATION>**'s cyber incident response steps and the phases set out in the NIST incident handling guide SP 800-61⁵ (the coloured blocks) is shown for reference.

***GUIDANCE – DELETE TEXT BOX UPON COMPLETION* - MANDATORY SECTION**

The fundamental steps for cyber incident response have been defined here. The nine-step lifecycle has been aligned to industry best practice and the Scottish Government recommendations. A flow diagram has been provided below as an example of the steps in the cyber incident response process.

<FLOW DIAGRAM TO GO HERE>

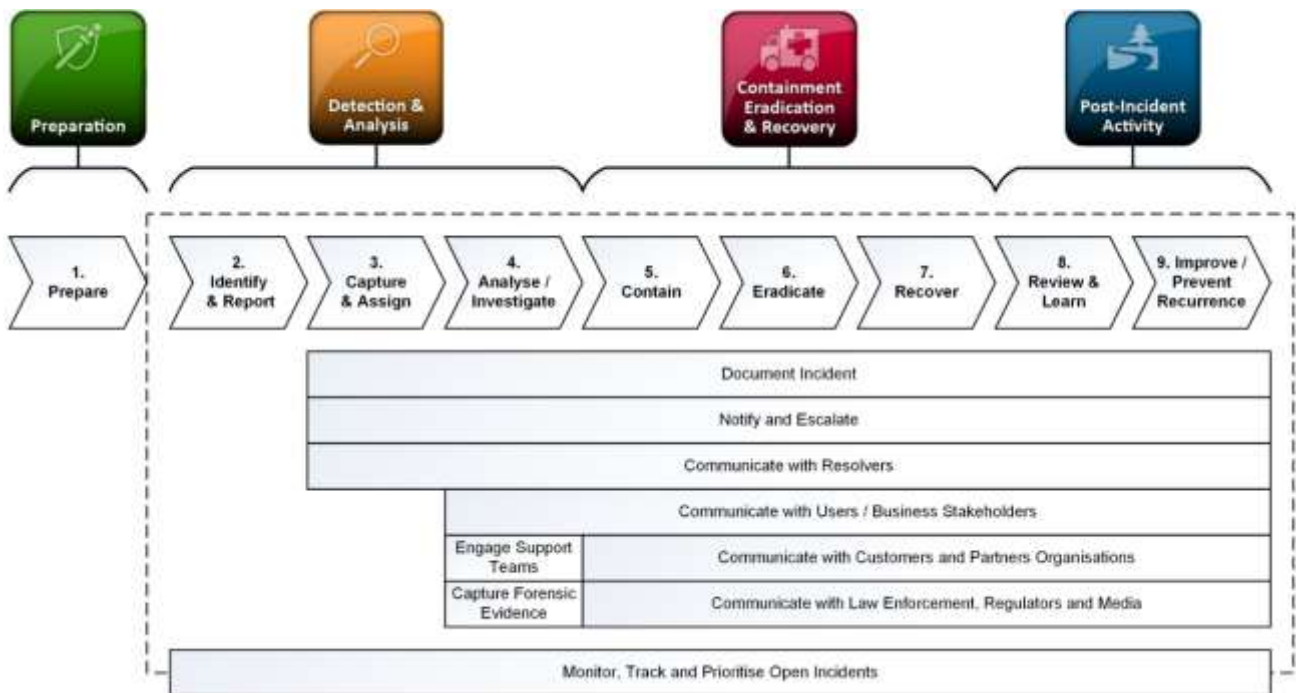


Figure 2 – Cyber Incident Response Process

⁵ Available here: <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf> (last visited 24th April 2019)

4.1 Step 1 – Prepare

***GUIDANCE – DELETE TEXT BOX UPON COMPLETION* - MANDATORY SECTION**

This section is based on industry best practices and NCC Group recommendations. Some preparation activities may vary but the content suggested below should be implemented as a minimum. The organisation may include additional preparation activities where necessary.

Section 4.1.1 lists recommended documentation that should be in place. It is understood that not all organisations will have the capacity to produce all of these documents, please use the list as a guidance for the type of documents to consider.

The key to minimising the impact and quickly recovering from a cyber incident is in the planning and preparation. A well trained team that has access to a comprehensive up-to-date set of documentation with a well-managed and monitored IT estate will greatly improve the response times to a cyber incident. Therefore the following actions should be undertaken in order to enable a CIRT to function effectively.

4.1.1 Required documentation

The documentation below must be comprehensive, easily accessible to those who require it and contained in a central location:

- Cyber incident Response Plan (this document)
- Detailed tactical workflows (Playbooks) for specific response actions
- Inventory of digital assets
- Network Diagrams
- Documentation of services, protocols, and ports allowed or links where this information resides
- Inventory of approved operating systems and applications
- Configuration standards for all systems
- Change control for all systems
- System logs
- Media inventory
- Detailed Forensic imaging procedures for all systems
- Contact information for:
 - Core IT CIRT members
 - CIRT members (Appendix B)
 - Crisis Management Team (CMT) members (Appendix C)
 - Third Party Support Providers (Appendix D)

4.1.2 Preparation

Gather Cyber Threat Intelligence to enable an understanding of the risks to the business and infrastructure, knowledge of threat actors, their motivation and delivery methods. Threat intelligence sources include:

- National Cyber Security Centre Threats reports
- Cyber Information Sharing Partnership (CiSP)
- Open source intelligence feeds, including security vendor assessments and security newsfeeds and subscriptions
- Police

Other preparatory activities include:

- Routinely review the <ORGANISATION> security architecture to ensure a comprehensive defensive structure is in place.
- Reviewing the organisations related policies e.g HR, DR, Business Continuity policies.

4.1.3 Pre-requisites

- Creation of known baselines for network, server, storage and application performance accounting for fluctuations in demand for known activities e.g. month end, product launch etc.
- Automated alerting from all systems when their performance or other metrics falls outside the acceptable tolerances
- Daily reviews of event logs
- Configuration Management Database (CMDB)
- Backup and recovery processes for all systems
- Ensure all system clocks are synchronised with a trusted network time source
- Implement a cohesive patch management plan for all operating systems and third-party applications
- Implement a functional vulnerability management program that identifies weaknesses in the <ORGANISATION> environment that can be efficiently remediated
- Develop and maintain relationships with law enforcement authorities
- Consider developing and maintaining partnerships with external third-parties for services such as:
 - Digital Forensics and other Incident Response services
 - Phishing site take-down
 - Cyber Insurance
 - Credit protection for data breaches
 - Customer call centre for use during a data breach
 - Crisis/reputation management
 - Threat Intelligence

4.1.4 Training & Awareness

- Annual CIRT training on cyber incident response plan actions
- Security awareness and incident response training course such as SANS MGT535 Incident Response Team Management

- Security awareness training is given to all staff as part of the induction process with annual refresher training. Incident detection and reporting
- Annual First Responder Training
- HR maintains a record of all staff security training

4.1.5 Testing

<ORGANISATION> shall execute a Testing, Training, & Exercise (TTX) program to sustain and refine the organisation's ability to handle cyber incidents in accordance with the best practices outlined in NIST Special Publication 800-84 Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities⁶. Testing should include:

- Annual penetration testing
- Annual Red Team testing (which could be used to test the incident response plan)
- 6 monthly internal testing of response plan / playbook, using simulated scenarios including:
 - Ransomware
 - Phishing
 - Distributed Denial of Service (DDoS)
 - Data loss and theft
- Testing of Insider threat assessment

⁶ Available at: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-84.pdf> (last visited 24th April 2019)

4.2 Step 2 & 3 – Identify and Report

***GUIDANCE – DELETE TEXT BOX UPON COMPLETION* - MANDATORY SECTION**

All organisations should have a process for the identification and notification of cyber incidents. This section should detail how a cyber incident is reported (e.g. through email or phone) and who this is reported to, in most organisations this will be the IT Service/Help Desk.

Key information that should be included when reporting an incident are detailed below, this is a minimum and should be adopted by all organisations.

Any suspected or actual breach of information security policy or systems must be immediately reported to the <ORGANISATION> Service/ Helpdesk by ORGANISATION specific. E.g phone email

In the event that a suspected breach involves a member of staff relating to a sensitive issue, then a report can be made directly to the <ORGANISATION RESPONSIBLE PERSON> or to the Head of your department.

<All systems will be monitored and have automated alerting enabled to create events of interest notifications when they fall outside the tolerances of the known baselines for performance.> ***GUIDANCE DELETE*** – This may not be applicable to all organisations.

When reporting a cyber incident, it is important to collect as much information about the incident as possible to enable the service desk to give the incident an initial priority. Key information to be captured should include:

- Contact information of the person reporting the incident and related parties
- Host names and IP addresses of suspected breached systems
- Nature of incident
- The potential impact of the incident along with which business area is likely to be affected by it
- Description of the activity and supporting evidence e.g. logs

Failure to report, log or respond to a notification of a cyber incident will be subject to the disciplinary procedures.

Once the above information has been obtained, this will allow the <ORGANISATION> Service/ Helpdesk to assign a priority to the incident. Using their workflow process, this will then determine whether this is a security incident and needs to be referred to the CIRT.

4.2.1 Incident Types

GUIDANCE – DELETE TEXT BOX UPON COMPLETION

The following table provides examples of cyber incidents. It is good practice to keep this in for general information.

Figure 3 below lists incident type and descriptions of the incident:

Ref.	Incident Type	Description
1	Installation or execution of unauthorised/malicious software.	Suspected, attempted or actual installation/execution of unauthorised or malicious software on a <ORGANISATION> device. Includes malware detections by anti-malware software (even if mitigated successfully) and detections by application whitelisting solutions.
2	Network intrusion, enumeration or other probe.	Suspected, attempted or actual network intrusion, enumeration or probe. Includes intrusion alerts generated by network security equipment such as firewalls or IDS/IPS.
3.1	Physical loss, theft or damage of an IT asset.	Suspected, attempted or actual physical loss, theft or damage of any IT asset containing <ORGANISATION> data. Includes the loss/theft of laptops, tablets, smartphones or removable media (USB sticks, CDs, DVDs, DATs, etc.).
3.2	Physical loss, theft or damage of hardcopy information.	Suspected, attempted or actual physical loss, theft or damage of any <ORGANISATION> information in hardcopy.
4	User impersonation (including account compromise/hijack).	Suspected, attempted or actual instances of user impersonation. Includes password-sharing, attacks on authentication controls, impossible log-on scenarios, zombie user accounts, etc.
5	Suspicious privilege amendment.	Suspected, attempted or actual instances where a genuine user appears to have been placed in an inappropriate user group or to otherwise have gained excessive privileges.
6	Suspicious use of legitimate privileges.	Suspected, attempted or actual instances where a user appears to have abused legitimate access privileges; e.g. by accessing a large number of files/records, e-mailing data to unauthorised recipients, copying data to removable media or unusual network locations, etc.
7	Eavesdropping on a legitimate communication channel.	Suspected, attempted or actual instances where <ORGANISATION> data appears to have been intercepted by an unauthorised party. Includes instances where sensitive data is transferred to authorised recipients in unencrypted form.
8	Service spoofing (e.g. MITM).	Suspected, attempted or actual instances where a data service belonging to, or used by, <ORGANISATION> is spoofed by a third party. Includes fake <ORGANISATION> websites.
9	Denial of Service / excessive resource consumption / spam).	Suspected, attempted or actual instances where an entity places an excessively high demand on a given information system or asset. Includes Denial of Service and spam.
10.1	Phishing	Suspected, attempted or actual instances where: <ul style="list-style-type: none"> Persons within <ORGANISATION> receive an email which claims to be something, or from someone, that it is not.

		<ul style="list-style-type: none"> Persons outside <ORGANISATION> receive an email which claims to be from or to otherwise represent <ORGANISATION>, but is not.
10.2	Social engineering	Suspected, attempted or actual instances where an unauthorised person attempts to gain access to <ORGANISATION> data or IT systems by deception or extortion of authorised users (staff, customers or third parties).
11	Inappropriate use of IT facilities (including inappropriate web browsing).	Suspected, attempted or actual instances where a user uses a system to which they have authorised access in a manner that is illegal, in breach of <ORGANISATION> policy or otherwise contrary to workplace norms. This includes: browsing websites that are inappropriate for the workplace; sending threatening, obscene or harassing communications; or accessing/storing illegal material (including in breach of copyright).
12	Other harmful mode not listed	Any event that is deemed to be a security event that falls within the remit of the CIRT, but which does not fall into any of the above categories.

Figure 3 – Incident Types

4.2.2 Data Classification

***GUIDANCE – DELETE TEXT BOX UPON COMPLETION* - MANDATORY SECTION**

Cyber incidents may have an impact on sensitive information. The following table provides an overview of the Government Security Classifications. If this does not apply to your organisation, ensure this is edited to align with data classification practices in your organisation.

<ORGANISATION> possesses and stores information with varying levels of sensitivity. If a cyber incident occurs, the response will depend on the type of data stored on the affected systems. The CIRT should review the Government Security Classifications⁷ for full guidance. Figure 4 below provides a high level summary for data classifications.

Classification	Description
OFFICIAL	The majority of information that is created or processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile. A limited subset of OFFICIAL information could have more damaging consequences (for individuals or the Government generally) if it were lost, stolen or published in the media. Where information is identified as such, it shall still be managed within the OFFICIAL classification tier, but shall attract additional measures (generally procedural or personnel) to reinforce the need to know. In such cases where there is a clear and justifiable requirement to reinforce the need to know, assets shall be conspicuously marked OFFICIAL – SENSITIVE .

⁷ Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf (last visited 24th April 2019)

SECRET	Very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors. For example, where compromise could seriously damage military capabilities, international relations or the investigation of serious organised crime.
TOP SECRET	HMG's most sensitive information requiring the highest levels of protection from the most serious threats. For example, where compromise could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations.

Figure 4 – Data Classifications

4.2.3 Reporting to the ICO

***GUIDANCE – DELETE TEXT BOX UPON COMPLETION* - MANDATORY SECTION**

Cyber incidents may necessitate reporting to external organisations including the NCSC, Police Government and Regulator or Competent Authority

In line with the GDPR (Article 33) the ICO must be informed within 72 hours of the organisation becoming aware of an incident resulting in a “risk to the rights and freedoms of those involved”.

The **CIRT/DPO/responsible person** shall determine whether the incident amounts to a data breach which requires to be reported to the ICO. Further guidance can be found at <https://ico.org.uk/>. For organisations working to the NIS Directive, further consideration is required to whether the incident meets the reporting thresholds for NIS Reporting to relevant the Competent Authority.

Where a decision to notify the ICO has been made, the following must be included as a minimum:

- Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned.
- Communicate the name and contact details of the contact point where further information can be obtained.
- Describe the likely consequences of the personal data breach.
- Describe the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

With regards to NIS Directive the Competent Authority will have pre-determined the specific reporting requirements to be followed.

Where an incident under investigation meets the reporting requirements of the Scottish Public Sector Cyber-Incident Central Notification and Co-ordination Policy, then core organisations including Police Scotland and the NCSC will have been informed and able to offer incident management and investigative support where appropriate. Where incidents fall below this policy position consideration will be given to informing the NCSC and Police Scotland of the incident. This decision will be taken by CIRT / responsible person.

Where the incident under investigation meets reporting requirement to the Regulator/ Competent Authority, then this be undertaken in line with organisational policy and guidance and approved by CIRT / responsible person.



4.3 Step 4 – Analyse and Investigate

***GUIDANCE – DELETE TEXT BOX UPON COMPLETION* - MANDATORY SECTION**

Analysis and categorisation of cyber incidents is a fundamental step in the cyber incident response process. The following section describes this process.

If your organisation has existing processes for the analysis and categorising of cyber incidents this should be included below but ensuring the basic principles are applied.

The **Core IT CIRT** will perform an initial triage and classification of all suspected cyber incidents to confirm the validity and the potential impact of the incident. The initial classification may be changed once more detailed investigation has been carried out. The initial classification should be retained so that this can be used to help refine and improve the overall incident response process.

- All incidents will be given an initial priority by the <ORGANISATION> Service Desk.
- All CIRT members will be emailed with details of the cyber incident.

Once an alert has been received, the **Core IT CIRT** must research the event, leveraging rapid data collection and initial analysis (triage). The goal of the triage is to acquire enough pertinent preliminary information to appropriately determine both the data classification involved and the estimated severity of the incident. The initial Incident Responder (initial entity to receive the alert or be assigned the alert) shall conduct an initial assessment and provide a data classification and a preliminary incident severity to the Incident manager. The **Core IT CIRT** should appropriately note and/or close out incidents involving false-positives according to the appropriate incident-tracking procedures. Where a confirmed incident meets the severity score is determined as **medium, high and critical**, it must be escalated to the CIRT.

4.3.1 Cyber Incident Severity Assessment

Incident severity as annotated in Figure 4 is guided by the consideration of two separate components: “Type of Threat” and “System/Information Criticality.”

4.3.1.1 Types of Threat

The following is an explicit description of these threats in descending order of criticality:

Types of Threat	Description
Threat Level 1	Human-Controlled Root-Level Compromise <ul style="list-style-type: none"> - Unauthorised external personnel (cyber intrusion). - Partner organisation exceeding authority. - Internal personnel exceeding authority.
	Close-Access Breach (physical penetration of a site) <ul style="list-style-type: none"> - Rogue wireless access point. - Router re-direct.
Threat Level 2	Human-Controlled User-Level Compromise <ul style="list-style-type: none"> - Unauthorised external personnel (cyber intrusion). - Partner organisation exceeding authority.

	- Internal personnel exceeding authority.
Threat Level 3	Automated (malware-controlled) Root-Level Compromise
Threat Level 4	Automated (malware-controlled) User-Level Compromise
Threat Level 5	Denial of Service
Threat Level 6	Focused Scanning or Unmanaged Malware

4.3.1.2 System/Information Criticality

The criticality of systems and information that is potentially at risk is the second component to guiding the assessment of the severity of an incident. The following is an explicit description of these system/information criticalities in descending order of importance:

System/Information Criticality	Description
Criticality Level 1	Enterprise-Wide Network Resources (Revenue-Generating Services, Routers, Switches, DNS, Proxies Firewall etc.).
Criticality Level 2	High Criticality Information – Confidential Information (Intellectual Property, PII, PHI etc.).
Criticality Level 3	High Criticality Systems (Active Directory, Exchange, Web Services etc.).
Criticality Level 4	Sensitive Information – Restricted Information (Sensitive Corporate Information, non-PII, Financial Transaction Information etc.).
Criticality Level 5	Non-Critical Multi-Use Systems (File Servers, SharePoint etc.).
Criticality Level 6	Individual Systems and Non-Sensitive Information.

4.3.1.3 Overall Incident Severity Score

The overall impact of these two components is established using the matrix below. To properly assess an Incident, place the components in the two axes of the below matrix, which provides an initial estimation of the Incident Severity.

System/Information Criticality	Incident Type					
	1	2	3	4	5	6
1	Critical	Critical	Critical	High	High	Medium
2	Critical	Critical	High	High	Medium	Medium
3	Critical	High	High	Medium	Medium	Medium
4	High	High	Medium	Medium	Medium	Low
5	High	Medium	Medium	Medium	Low	Low
6	Medium	Medium	Medium	Low	Low	Low

Figure 4 – Incident Severity Assessment Matrix

4.3.1.4 Incident Severity Guidance

***GUIDANCE – DELETE TEXT BOX UPON COMPLETION* - MANDATORY SECTION**

Using the incident severity assessment matrix determines an overall severity classification. This will dictate how a cyber incident will be responded to. Below are four recommended incident severity classifications. The impact can be tailored to your organisation, providing an example of consequences to consider. If your organisation has existing processes for the classification of cyber incidents, ensure this is included to maintain consistency within your organisation.

The following guidelines are for categorising the severity of an incident based on the known facts of the incident and the subsequent impact to the organisation. The prioritisation of how to resource the response to the incident is a critical decision point in the process. The CIRT should handle incidents based upon the risk they pose to <ORGANISATION>, its information, and computing environment. This section describes the severity levels within <ORGANISATION>, and the structure that is used to determine this.

The Core IT CIRT will normally handle severity levels assessed as **LOW**, whilst the CIRT will normally handle severity cases assessed as **MEDIUM**, **HIGH** and **CRITICAL**

Severity Level	Impact to <ORGANISATION>	Incident Response Characteristics
CRITICAL	<p>Highest severity level. Impacts are extraordinary and potentially catastrophic to the proper conduct of <ORGANISATION'S> business, loss of public trust, and/or impact on <ORGANISATION> operations or personnel. Impacts that are indicators of this degree of severity are:</p> <ul style="list-style-type: none"> • Threat to life or physical safety of the public, customer, or <ORGANISATION> personnel. • Significant destruction of IT systems/applications. • Significant destruction of corporate capabilities. • Significant disruption of <ORGANISATION> business operations over a sustained period of time. • Massive loss of confidential information. Significant loss of public confidence. • Dramatic reputational damage. • Risk of financial loss (generally more than £500,000). 	<p>This level requires immediate and continual response actions from the <ORGANISATION> CIRT. An incident of this severity has the most significant impact on <ORGANISATION> operations and involves an extensive, persistent, and usually very sophisticated attack that is difficult to contain, control, or counteract. This level of severity will trigger the Scottish Public Sector Cyber Incident Central Notification and Co-ordination Policy.</p> <p>Indicators of this are:</p> <ul style="list-style-type: none"> • Executive leadership and the company Board of Directors will have an immediate and ongoing interest in the incident, the investigation, and the eventual recovery from the incident. • Major external support from multiple organisations would be engaged. • Would likely involve law enforcement. • Would likely involve multiple levels of regulatory or compliance reporting. • Would likely involve engagement by multiple media outlets.
HIGH	<p>Impacts are substantial to the proper conduct of <ORGANISATION> business, loss of public trust, and/or impact on <ORGANISATION> operations or personnel. Impacts that are indicators of this degree of severity are:</p> <ul style="list-style-type: none"> • Impactful destruction of some IT systems/applications. • Impactful destruction of some corporate capabilities. • Substantial disruption of <ORGANISATION> business operations over a sustained period of time. • Substantial loss of confidential information. • Substantial loss of restricted information. • Substantial loss of public confidence. • Substantial reputational damage. 	<p>This level requires immediate response from the Core CIRT. The Extended CIRT must also be notified. Most of the Extended CIRT will likely be engaged at some point of the incident response effort. This level may involve extended work hours, to include weekends, or could involve 24/7 response activities. An incident of this severity has a real and negative impact on <ORGANISATION> operations and involves a persistent or sophisticated attack that requires substantial resources to contain, control, or counteract. This level of severity will trigger the Scottish Public Sector Cyber incident Central Notification and Co-ordination Policy.</p> <p>Indicators of this are:</p> <ul style="list-style-type: none"> • Executive leadership and the company Board of Directors will likely have an interest in the outcome of the incident, the investigation, and the eventual recovery from the incident.

	<ul style="list-style-type: none"> • Risk of financial loss (generally between £100,000 and £500,000). 	<ul style="list-style-type: none"> • External support from multiple organisations will likely be needed to resolve. • Would likely involve law enforcement. • Would likely involve some level of regulatory or compliance reporting. • Would likely involve engagement by some media outlets.
<p>MEDIUM</p>	<p>Impacts are moderate to the proper conduct of <ORGANISATION> business, and/or impact on <ORGANISATION> operations or personnel. Impacts that are indicators of this degree severity are:</p> <ul style="list-style-type: none"> • Moderate disruption of <ORGANISATION> business operations over a sustained period of time. • Multiple sites or multiple business units affected by the incident. • Moderate loss or manipulation of restricted information. • Limited loss of public confidence. • Limited reputational damage. • Risk of financial loss (generally between £25 and £100,000). 	<p>This level requires notification to the <ORGANISATION> CIRT. Several or most <ORGANISATION> CIRT members will be engaged in some aspect of the response effort. The Extended CIRT must also be notified. Selected Extended CIRT members may be engaged at some point of the incident response effort. This level may involve extended work hours initially, and will revert to a normal working schedule once initially contained. An incident of this severity has some impact on <ORGANISATION> operations and involves an attack that requires an organized response to contain, control, or counteract. This level of severity will trigger the Scottish Public Sector Cyber incident Central Notification and Co-ordination Policy.</p> <p>Indicators of this are:</p> <ul style="list-style-type: none"> • External support may be needed, and will be engaged as needed. • May involve law enforcement. • May involve some limited level of regulatory or compliance reporting. • Would likely not involve media outlets.

LOW	<p>Impacts are greatly limited to the proper conduct of <ORGANISATION> business, and/or impact on <ORGANISATION> operations or personnel. Impacts that are indicators of this degree severity are:</p> <ul style="list-style-type: none"> Limited or no disruption of <ORGANISATION> business operations. One site or business unit affected by the incident. Limited or no unauthorised access to restricted information. No impact to public confidence. No impact to reputation. Risk of financial loss (Under £25,000). 	<p>This level requires handling by a cyber or incident response team member (Core IT CIRT) and some Extended CIRT members may be notified if deemed necessary. This level of response is conducted during normal working hours. An incident of this severity has limited or no impact on <ORGANISATION> operations. Indicators of this are:</p> <ul style="list-style-type: none"> External support is generally not needed. Law enforcement is generally not engaged. Regulatory reporting is not warranted. Would likely not involve media outlets.
------------	---	---

Figure 5 – Incident Severity Assignments

4.3.1.5 Key Escalation Contacts

Contact	Details
The Scottish Government Cyber Resilience Unit (CRU)	Email: cyberresilience@gov.scot Phone: 0300 244 4000 ask for duty CRU Officer,
Police Scotland	Email: C3DivisionServiceOverview@scotland.pnn.police.uk Phone: dial 101 ask for Duty Cyber Officer
SGoRR	Email: SGORRInformation@gov.scot Pager: 07623 514719 (pager) ask for SGoRR Duty Officer
NCSC Incidents Team	Email: Incidents@ncsc.gov.uk Phone: 3000 200 973
External Contracted Cyber Partner	

4.4 Step 5 – Containment

***GUIDANCE – DELETE TEXT BOX UPON COMPLETION* - MANDATORY SECTION**

Steps 5 – 9 are based on NCC Group experience and industry best practice, it is recommended that these sections remain and be implemented by the organisation.

The CIRT or Core IT CIRT will take actions to contain and isolate the incident from the corporate network; this may include the following:

- Isolating a system from the corporate network
- Removing users access privileges
- Removing users from the corporate offices
- Stopping services running
- Isolating connections to external partner's networks to prevent spread to other organisations
- Identifying systems and services affected including details of:
 - Host names,
 - IP addresses,
 - MAC addresses,
 - Active services,
 - Locations
- Identifying times and source IP addresses of the attack including the following details
 - Host names,
 - IP addresses,
 - MAC addresses,
 - Protocols,
 - Locations,
 - Time,
 - User accounts used
- If required contact specialist external support services to assist in the containment and evidence gathering.

Details of handling procedures for specific attacks, including DDoS, Hacking, Suspicious Activity (virus or malware, loss or theft of data) are detailed in the **<ORGANISATION PLAYBOOKS>**.

Handling procedures for forensic evidence

GUIDANCE – DELETE TEXT BOX UPON COMPLETION

Forensic handling procedures should be properly recorded for your organisation. If in any doubt, advice should be sought from Police Scotland specialists on handling evidence.

- Maintain the state of the affected system (i.e. do not power off)
- Identify all potential sources of available evidence which may include:
 - Storage media (HDD, DVD, USB, Tape)
 - Live data (RAM, IM, network connections, encrypted files and folders)
 - Application data (temporary files and folders, browser history, email, images, swap file, hibernation files)
 - Servers (active directory, email, internet server, web server, encryption key distribution, authentication servers);
 - Logs (event, traffic, AV, software)
 - Mobile phones (call history, contacts, emails, photos, videos, SMS, calendars, locations)
 - Sat Nav (journeys, locations)
 - Electronic Files (documents, databases, spread sheets, PDFs, presentations)
 - Hard files (printed copies, bills, invoices, receipts, notes, diaries)
 - Meta data (dates, times, authors, accessed, created)
- Log all actions taken including:
 - Name, date and time of the person collecting the evidence
 - How the evidence was collected, preserved, duplicated, analysed and stored
 - If possible have a witness to the process of the forensic evidence being taken.
 - Secure system logs to prevent them being overwritten or deleted until the security incident has been closed.
 - If relevant, undertake forensic copies from computer memory to a file, and take a back-up of the file;
 - If relevant, take a forensic image (copy) of the computer hard drive(s), which will be used for further analysis, to ensure that the evidence on the original system is unharmed;
 - Forensic evidence of a breach or suspected breach must be secured within 24 hours.
 - Forensic evidence must only be gathered by trained personnel or specialist third parties
 - Untrained personnel must not attempt to gather forensic evidence

A forensic imaging guide has been provided within Appendix B for the purpose of forensically preserving data.

****If in any doubt advice should be sought from Police Scotland specialists on handling evidence.***

4.5 Step 6 – Eradicate

MANDATORY SECTION

The objective of the eradicate step is to:

- Correct the incident by addressing its symptoms (e.g. healing malware infections or correcting access control lists).
- Prevent its immediate reoccurrence by addressing its root cause. For example: changing networking rulesets, moving the target host to a different network segment and/or IP address, or constraining access to the target data to the minimum possible subset of users.
- Cyber Incident Playbooks provide details of eradication considerations for specific attacks and should be referred to as appropriate

4.6 Step 7 – Recovery

MANDATORY SECTION

Actions can be taken to restore services back to the pre-incident state once the CIRT or Core IT CIRT confirm the remediation actions have been successful. However careful monitoring of the estate should be taken to ensure any vulnerabilities have been successfully closed. The recovery actions will include the following:

- Ensure that the impacted services are accessible again
- Ensure performance is in line with known (pre-attack) baseline
- Switch back traffic to the original network
- Restart stopped services
- Continue to monitor the performance/activities of the affected systems
- Confirm application behaviour is as expected
- Conduct vulnerability scan if deemed appropriate

4.7 Step 8 & 9 – Reporting and Lessons Identified

MANDATORY SECTION

All cyber incidents will have a cyber incident report created. Cyber incidents will be fully reported and reviewed within 5 days of the incident resolution. Summary reports of all incidents will be reviewed at a **Monthly** meeting chaired by the CISO who will decide on actions to take forward from the cyber incident report.

A cyber incident review is important so the business and CIRT can improve the systems and procedures to reduce the impact of future cyber incidents.

Where external partners have been involved in the incident management process, consideration should be given to their involvement in the post incident debrief (which will form the lessons identified). Where appropriate the Resilience Lead will be tasked with sharing the lessons identified with the wider Resilience Partnerships through the Local and Regional Partnership structures.

Details to be captured in a cyber incident report include:

- How and when the incident was initially detected
- How and when the incident was initially classified
- List of people notified
- Actions and timelines of CIRT
- Whether any internal and/or external escalation was required
- List positive and negative points of the response to the incident
- Estimated cost of the incident; including loss of revenue to the business, internal and external resource costs, legal costs and fines. The full details may not available within 5 days of the incident resolution. Further review may be required 6 months from the resolution of the incident
- Whether the incident led to disciplinary action or prosecution. As above, legal and disciplinary actions will take longer than the 5 days to resolve, therefore, initial comments will be adequate at this point. Further review may be required 6 months from the resolution of the incident
- Lessons identified
- Recommendation for improvements to policy, procedure, systems and services
- Could any technical controls be implemented to prevent reoccurrence
- Implementation plan for the identified improvements to the plan

Following the publication of a given Incident Report, the **<ORGANISATION RESPONSIBLE PERSON>** shall:

- Seek recipient feedback in relation to the incident report
- Confirm the viability of each security control change/addition recommended in the incident report
- Identify the approximate cost of, and timeframe for, delivering each security control change/addition recommended in the report which appears viable (i.e. to which report recipients did not object)
- Identify a proposed action owner and action target date for delivering each proposed recommendation
- Identify the proposed funding route for each proposed recommendation that requires financial expenditure
- Seek the **<ORGANISATION CISO OR RESPONSIBLE PERSON>**'s (and, where actions fall outside of **<ORGANISATION IT DIRECTOR/GROUP IT>**) endorsement of the proposed actions and associated funding routes

- Seek the action owner's acceptance of the relevant actions and target dates
- If action owner acceptance of the proposed actions is not forthcoming, escalate to the <ORGANISATION CISO OR RESPONSIBLE PERSON>'s (and, in the case of actions falling outside of <ORGANISATION IT DIRECTOR/GROUP IT>)
- Review, at not less than monthly intervals, progress with each action with each action owner
- Notify the <ORGANISATION CISO OR RESPONSIBLE PERSON>'s of any action at risk of not being delivered prior to its target date
- Consider sharing the lessons identified with appropriate external partners, including but not limited to Police Scotland, Scottish Government (CRU and lead Policy team), Resilience Partnerships, SGoRR, ScoRDS and NCSC

5. Appendix A – Forensic Imaging Guide

The steps listed below are a guide to assist in the capture of forensic images. Forensic evidence must only be gathered by trained personnel. Failure to follow the correct procedure when creating a forensic image can result in the image being inadmissible as evidence

- If a forensic bridge/write blocker is available, remove the HDD from the machine and attach it to the write blocker which in turn is connected to an imaging machine. Proceed to take a forensic image using forensic imaging software which should be installed on the imaging machine and refer to the official user guide if required
- If a forensic bridge is unavailable or it is impractical to remove the HDD from the machine then boot the machine to a live Linux distribution, such as Raptor v3.0. Ensure that the boot options are known for that particular machine and that the BIOS is configured to allow booting from USB or disc. To help ensure Windows does not boot if the live boot is missed, be prepared to disconnect from the power immediately (always remove the battery from laptops)
- Once successfully booted, the imaging wizard should automatically launch. Attach a destination drive where the forensic image is to be copied to and proceed to image using the wizard and refer to the official Raptor user guide if required
- For both forensic imaging software and Raptor, ensure the verification option is checked and hash values produced (see image on next page)
- Enter the machine's BIOS settings and record (take photo) as a minimum of the system clock settings
- For cases involving theft, fraud, computer misuse, unauthorised access and other cases involving where the user is under investigation, check optical drives for discs, USB ports for other media which should be labelled, placed in an evidence bag and placed in locked storage pending an investigation. Do NOT browse these devices live
- If unable to capture a forensic image using the provided tools secure the device and seek advice from Head of IT as soon as practically possible as third parties may need to be informed
- Do NOT boot the machine and perform a live analysis unless all other methods have been exhausted and advice sought from the Head of IT
- If the infected machine is offshore/remote, instruct the user accordingly:
 - For malware, remove from the network. If forensic imaging software is available instruct the user how to image RAM and hard drive, disconnect power and return the machine and RAM/drive image to IT for further imaging and analysis
 - For other types of investigation, such as misuse, inform a line manager to disconnect the power and seize the machine for return to IT, ensuring all actions have been recorded and that no one interferes with the evidence

If the suspected user(s) is no longer an employee and the machine is not in use, consider seizing and place in an evidence bag after a forensic image has been captured, record all details and place in locked storage.

If the machine needs to be re-introduced into the business (i.e. issued to another user) the HDD should be removed and placed in an evidence bag, then a new HDD placed in the machine ready for re-issue. If not then the HDD must be securely erased rather than simply formatting and re-building with the corporate image.

If the machine is currently in use by another user, capture a forensic image (RAM not required) and record details of when the new user came into possession of the machine.

Virtual servers – Forensic image is not required, but obtain a snapshot or clone (VMSN, VMDK) for investigation and reset to last known good state

6. Appendix B – Cyber Incident Response Team (CIRT) Contact

GUIDANCE – DELETE TEXT BOX UPON COMPLETION

Appendix B, C and D must be tailored by the organisation completing the template. Each section has recommended roles. These may vary per organisation. Most importantly these contacts should be regularly reviewed and a nominated person assigned to ensure up to date and relevant.

Information

Name	Job Role	Email	Phone	Office Hours
<ORGANISATION TAILORED SECTION>	[Head of IT]	Work: Personal:	Office: Mobile: Home:	
	[Head of Architecture & Security]	Work: Personal:	Office: Mobile: Home:	
	[Head of Infrastructure & Support]	Work: Personal:	Office: Mobile: Home:	
	[Head of Business Systems Development]	Work: Personal:	Office: Mobile: Home:	
	[IT Governance Manager]	Work: Personal:	Office: Mobile: Home:	
	[Business Unit Manager]	Work: Personal:	Office: Mobile: Home:	
	[Business Unit Manager]	Work: Personal:	Office: Mobile: Home:	
	[Board/Senior Mgt member responsible for cyber resilience]			
	[HR]	Work: Personal:	Office: Mobile: Home:	
	[Legal]	Work: Personal:	Office: Mobile: Home:	
	[Finance]	Work: Personal:	Office: Mobile: Home:	
	[Policy Lead]	Work: Personal:	Office: Mobile: Home:	
	[Resilience Lead]	Work: Personal:	Office: Mobile: Home:	
	[Business Continuity Lead]	Work: Personal:	Office: Mobile: Home:	



7. Appendix C – Crisis Management Team (CMT) Contact Information

Name	Job Role	Email	Phone	Office Hours
<ORGANISATION TAILORED SECTION>	[CRO]	Work: Personal:	Office: Mobile: Home:	
	[CFO]	Work: Personal:	Office: Mobile: Home:	
	[IT Director]	Work: Personal:	Office: Mobile: Home:	

8. Appendix D – Third Party Support Services Contact Information

Supplier	Description of Services	Contact	Email	Phone
<ORGANISATION TAILORED SECTION>	[IT Support]	Work: Personal:	Office: Mobile: Home:	
	[Data Centre]	Work: Personal:	Office: Mobile: Home:	
	[ISP / DNS Management]	Work: Personal:	Office: Mobile: Home:	
	[Hosting]	Work: Personal:	Office: Mobile: Home:	
	[Software Developers]	Work: Personal:	Office: Mobile: Home:	
	[Forensic Services]	Work: Personal:	Office: Mobile: Home:	
	[Legal Counsel]	Work: Personal:	Office: Mobile: Home:	
	[Press and PR]	Work: Personal:	Office: Mobile: Home:	
	[Police]	Work: Personal:	Office: Mobile: Home:	
	[IT Support]	Work: Personal:	Office: Mobile: Home:	

9. Appendix E – Scottish Public Sector Cyber Incident Central Notification and Coordination Policy

The above policy is subject to change and the version as on August 2019 is contained within the following embedded pdf



CYBER--2.PDF

10. Appendix F – Notifiable Reporting Form

Notifiable Scottish Public Sector Cyber Incidents are defined as incidents or attacks against Scottish public sector network information systems which:

- *have the potential to disrupt the continued operation of the organisation or delivery of public services; and/or*
- *carry a likelihood that other public, private or third sector organisations may experience a similar attack, or that the incident could spread to those organisations; and/or*
- *could have a negative impact on the reputation of the Scottish public sector or Scottish Government; and/or*
- *carry the likelihood of Scottish Parliament or national media interest.*

Scottish public sector organisations who are impacted by notifiable cyber incidents should complete the notifiable cyber incident reporting form below as early as possible and, if email services are available, send the completed form simultaneously to the following addresses in addition to those relevant to your own organisational requirements:

- The National Cyber Security Centre (NCSC): Incidents@ncsc.gov.uk
- The Scottish Government Cyber Resilience Unit (CRU): cyberresilience@gov.scot
- Police Scotland: C3DivisionServiceOverview@scotland.pnn.police.uk
- SGOR: SGORRInformation@gov.scot

These services are available 24 hours a day, 7 days a week, and can be contacted at any time in the event of a notifiable cyber incident. The 'follow up' numbers are as follows:

- The National Cyber Security Centre (NCSC): 03000 200 973
- The Scottish Government Cyber Resilience Unit (CRU): 0300 244 4000, ask for CRU Duty Officer
- Police Scotland : 101 and ask for the Cyber Crime Unit On Call Officer
- SGoRR: 07623 514719 (pager) SGoRR Duty Officer

Where public sector organisations are aware that sector / network-specific co-ordinating bodies also have an interest, or role to play, in a notifiable cyber incident, they should copy these bodies into the email.

In the event that any central co-ordinating body (SG CRU, Police Scotland, NCSC) is notified of a notifiable cyber incident involving a Scottish public sector organisation that has not been reported through the "Report it Once and Follow Up" procedure outlined above, it will seek agreement from the organisation affected to inform the other central coordinating bodies and sector/network-specific coordinating bodies.



PLEASE DO NOT FILL THIS FORM IN ON ANY NETWORK YOU BELIEVE HAS BEEN COMPROMISED. USE A SEPARATE SYSTEM TO FILL THIS IN.

Your Name

Your Phone

Your Contact Email Address

(The email address from an **uncompromised** system that all further correspondence should be sent to.)

Your Company Email Address

(The company email address for reference purposes (this may be compromised, but will not be used for correspondence)

What Organisation are you reporting an incident for?

What is your Role?

Summary of Incident

Are you sharing this with us for information or do you require advice and assistance from Police Scotland (investigation) NCSC (Incident Management) or SG CRU (Ministerial awareness or threat sharing)

If assistance please specify

Do you have an Internal ID for the incident?

Investigation so far



Impact

- Select -

Description of Impact

Empty text area with scrollbars

Current state of incident

- Select -

Notification:

Have you reported this to:

Scottish Government Cyber Resilience Unit? Yes No

NCSC? Yes No

Police Scotland? Yes No

Information Commissioner’s Office (ICO) as a GDPR obligation? Yes No N/A

Relevant Competent Authority (CA) as a NIS Directive obligation? Yes No N/A

Who else has been notified?

Empty text area with scrollbars

e.g external specialist response providers, Resilience Partners

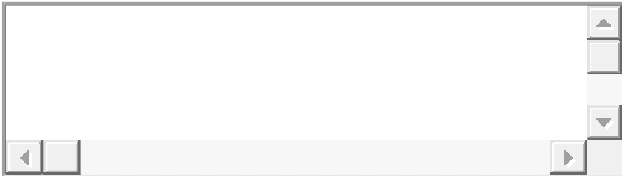
Do you have any further data or samples to aid this incident? Yes No

Information Sharing:

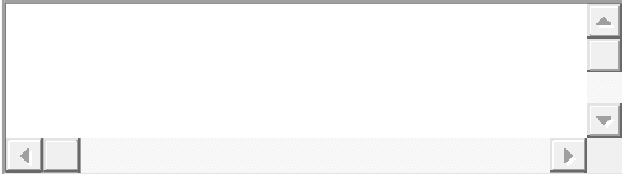
Has any information been shared on the CISP? Yes No

Do you have information you wish to have shared across the CREW network ? Yes No

If yes please provide the message content providing information that would enable other network defenders to take mitigating action.

An empty rectangular text box with a light gray background and a thin black border. It features a vertical scrollbar on the right side and a horizontal scrollbar at the bottom.

Are there Media lines prepared is so can they be provided below?

An empty rectangular text box with a light gray background and a thin black border. It features a vertical scrollbar on the right side and a horizontal scrollbar at the bottom.

11. Appendix G – NCSC Incident Categorisation Framework

NCSC defines the following:

Cyber-attack: Attempts to damage, disrupt or gain unauthorised access to computer systems, networks or devices.

Small & medium sized organisations: Businesses, charities, clubs and schools with up to 250 employees. Likely to not have a dedicated team managing cyber security.

Large organisations: Businesses, charities and critical national infrastructure with more than 250 employees. Likely to have a dedicated team managing cyber security.

Category	Category definition	Who responds?	What do they do?
Category 1 National cyber- emergency	A cyber-attack which causes sustained disruption of UK essential services or affects UK national security, leading to severe economic or social consequences or to loss of life.	Immediate, rapid and coordinated cross-government response. Strategic leadership from Ministers / Cabinet Office (COBR), tactical cross-government coordination by NCSC, working closely with Law Enforcement. Scottish Government Resilience Room (SGoRR) activated and would take a co-ordination role working with COBR.	Coordinated on-site presence for evidence gathering, forensic acquisition and support. Co-location of NCSC, Law Enforcement, Lead Government Departments, Devolved Administrations and others where possible for enhanced response. SGoRR undertakes multi agency co-ordination role in Scotland.
Category 2 Highly significant incident	A cyber-attack which has a serious impact on central government, UK essential services, a large proportion of the UK population, or the UK economy.	Response typically led by NCSC (escalated to COBR if necessary), working closely with Law Enforcement as required. Cross-government response coordinated by NCSC. SGoRR activated and would take a leading co-ordination role working with COBR if activated. SG CRU would act as the interface with the NCSC.	NCSC will often provide on-site response, investigation and analysis, aligned with Law Enforcement criminal investigation activities. SGoRR undertakes multi agency co-ordination role in Scotland. SG CRU acts as the interface with the NCSC.
Category 3 Significant incident	A cyber-attack which has a serious impact on a large organisation or on wider / local government, or which poses a considerable risk to central government or UK essential services.	Response typically led by NCSC, working with Law Enforcement as required. SGoRR likely to be activated and would take a leading co-ordination role. SG CRU would act as the interface with the NCSC.	NCSC will provide remote support and analysis, standard guidance; on-site NCSC or Law Enforcement support may be provided. SGoRR undertakes multi agency co-ordination role in Scotland. SG CRU acts as the interface with the NCSC.

<p>Category 4 Substantial incident</p>	<p>A cyber-attack which has a serious impact on a medium-sized organisation, or which poses a considerable risk to a large organisation or wider / local government.</p>	<p>Response led either by NCSC or by Law Enforcement dependent on the incident. SGoRR may be activated and, if so, would take a leading co-ordination role. SG CRU would act as the interface with the NCSC.</p>	<p>NCSC or Law Enforcement will provide remote support and standard guidance, or on-site support by exception. SGoRR (if activated) undertakes multi agency co-ordination role in Scotland. CRU acts as the interface with the NCSC.</p>
<p>Category 5 Moderate incident</p>	<p>A cyber-attack on a small organisation, or which poses a considerable risk to a medium-sized organisation, or preliminary indications of cyber activity against a large organisation or the government.</p>	<p>Response led by SG CRU, Law Enforcement working with Organisation as appropriate SG CRU working with Lead Policy Area to provide co-ordination role, inc. considering Ministerial briefing and intelligence sharing opportunities.</p>	<p>Law Enforcement will provide remote support and standard guidance, with on-site response by exception. Scottish Government CRU working with Lead Policy Area to co-ordinate briefings to Scottish Ministers encourage intelligence sharing, and accessing appropriate advice and guidance from NCSC and Police Scotland.</p>
<p>Category 6 Localised incident</p>	<p>A cyber-attack on an individual, or preliminary indications of cyber activity against a small or medium-sized organisation.</p>	<p>Response led by SG CRU, Law Enforcement working with Organisation as appropriate SG CRU working with Lead Policy Area to provide co-ordination role, inc. considering Ministerial briefing and intelligence sharing opportunities</p>	<p>Remote support and provision of standard advice. On-site response by exception. Scottish Government CRU working with Lead Policy Area to co-ordinate briefings to Scottish Ministers encourage intelligence sharing, and accessing appropriate advice and guidance from NCSC and Police Scotland.</p>

12. Appendix H – List of Abbreviations

Abbreviation	Meaning
CIRP	Cyber incident Response Plan
CIRT	Cyber incident Response Team
CISO	Chief Information Security Officer
CiSP	Cyber Information Sharing Partnership
CMDB	Configuration Management Database
CMT	Crisis Management Team
COBR	Cabinet Office Briefing Rooms
CONOPS	Concept of Operations
CRO	Chief Risk Officer
DDOS	Distributed Denial of Service
DNS	Domain Name System
DPO	Data Protection Officer
HR	Human Resources
ICO	Information Commissioner's Office
IP	Internet Protocol
ISM	Information Security Manager
IT	Information Technology
MAC	Media Access Control
MITM	Man in the Middle
NCIMP	National Cyber incident Management Policy
NCSC	National Cyber Centre
NIST	National Institute of Standards and Technology
RACI	Responsible / Accountable / Consulted / Informed
SG CRU	Scottish Government Cyber Resilience Unit
SGoRR	Scottish Government Resilience Room
SIEM	Security Information and Event Management
SPoC	Single Point of Contact
TTX	Testing, Training, & Exercise