Cyber Incident Response Plan

<organisation name>

Contact the Victorian Government Cyber Incident Response Service for assistance in responding to cyber incidents. Contact 1300 CSU VIC or cybersecurity@dpc.vic.gov.au

Cyber Incident Response Plan

<organisation name>

Contents

1. Introduction 3
   - 1.1 Context 3
   - 1.2 Purpose 3
   - 1.3 Authority 3
   - 1.4 Review 3
2. Terminology and Definitions 4
3. Common Cyber Incidents and Responses 5
   - 3.1 Potential Threat Vectors 5
4. Roles and Responsibilities 6
   - 4.1 Incident Management Team 6
5. Incident Response Process 8
   - Step 1: Detection and Analysis 8
   - Step 2: Containment and Eradication 13
   - Step 3: Communications and Engagement 15
   - Step 4: Recover 16
   - Step 5: Learn and Improve 16
   - Appendix A. Situation update (template) 18
   - Appendix B. Incident Log (template) 19
   - Appendix C. Resolution action plan (template) 20
   - Appendix D. Evidence register (template) 21
   - Appendix E. Assets and key contacts (template) [update as appropriate] 22

IMPORTANT

Before activating this cyber incident response plan it is important that you update the document to include information specific to your organisation and its cyber security operating environment.

Populate the document with details of key contacts, incident management team members, critical assets, organisational policies/procedures and other security-related information.

REMOVE THIS TEXT BOX BEFORE FINALISING THE PLAN

1. Introduction

1.1 Context

Cyber security relates to the confidentiality, availability and integrity of information and data that is processed, stored and communicated by electronic or similar means, and protecting it and associated systems from external or internal threat.

It is commonly recognised that cyber security involves the protection of critical information and ICT infrastructure, including supervisory control and data acquisition (SCADA) systems and industrial control systems (ICS), through the alignment of people, processes and tools.

As the technology that underpins ICT infrastructure and related systems is continually advancing, cyber criminals are also advancing their skills and exploiting technology to conduct cyber-attacks with the aim of defrauding funds, disrupting business or committing espionage. Furthermore, advanced technology is also complex, which leads to human error and workflow mistakes such as misconfigurations and general cyber security behaviours that do not meet best practice.

This document supports <organisation> in managing contemporary cyber threats and incidents. The application of this document will support <organisation> in reducing the scope, impact and severity of cyber incidents.

1.2 Purpose

This document describes the process that is required to ensure an organised approach to managing cyber incidents within <organisation> and coordinating response and resolution efforts to prevent or limit damage that maybe caused.

This document is developed using the National Institution of Standards and Technology (NIST) Computer Security Incident Handling Guide.

1.3 Authority

This cyber incident response plan is managed by <team/person managing the plan>. This plan has been endorsed by <relevant authority> who is responsible for ensuring that <organisation> has a dependable and secure ICT environment.

1.4 Review

This incident response plan will be reviewed annually by <team/person managing the plan>, or following any cyber incident as deemed necessary by <organisation>.

2. Terminology and Definitions

This section outlines key terminology and definitions used in this plan.

2.1.1 What is a cyber event?

A cyber event has the potential to become, but is not confirmed to be, a cyber incident.

Examples of cyber events include (but are not limited):

- Multiple failed sequential logons for a user
- A user has disabled the antivirus on their computer
- A user has deleted or modified system files
- A user restarted a server
- Unauthorised access to a server or system.

2.1.2 What is a cyber incident?

A cyber incident occurs when there is a breach of explicit or implied digital security policy that requires corrective action because it threatens the confidentiality, availability and integrity of an information system or the information the system processes, stores or transmits.

Examples of cyber incidents include (but are not limited to):

- Denial of service attacks (DoS) that affect system or service availability
- Virus or malware outbreak (including ransomware)
- Compromise or disclosure of sensitive or personal information
- Compromise of network credentials or an email account.

This plan identifies four categories of cyber incidents which are differentiated by the level of impact they create.

3. Common Cyber Incidents and Responses

The following table provides a list of common cyber incident types, along with the corresponding response activities (which form the typical minimum response).

#	Type / Description	Initial response to minimise potential harm
1	**Ransomware**; a tool used to encrypt or lock victims' data until a ransom is paid.	Immediately remove the infected device(s) from the network to limit the spread of ransomware. Capture all available logs relevant to the device. Isolate the devices while containment and eradication activities are determined.
2	**Malware Infections**; a virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host.	Immediately remove the infected device(s) from the network to limit the spread of malware. Capture all available logs relevant to the device. Isolate the devices while containment activities are confirmed and eradication efforts are determined.
3	**Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks**; overwhelming an ICT network with traffic that it cannot process, sometimes causing the network to fail.	Request gateway services provider to identify DOS/DDOS nature, attack vector and implement suitable solutions. Liaise with gateway services and network team to apply filters at network edge and / or increase capacity.
4	**Phishing and Social Engineering**; deceptive communications designed to elicit users' sensitive information (including network credentials).	Review logs of affected users (web and email logs) to determine whether malicious links/attachments were accessed. Consult users to confirm what actions they took, and whether any personal/sensitive information was provided in response to a phishing/social engineering attempt. Consider resetting user passwords and monitoring accounts for any unauthorised access.
5	**Data breach**; unauthorised access to sensitive or personally identifiable information.	Contain the data loss/spill as soon as possible. Alert privacy, legal and communications/media teams. Investigate the cause of the data loss/spill.

3.1 Potential Threat Vectors

There are multiple vectors through which a cyber incident can arise. Maintaining awareness of these threat vectors will support <organisation> in identifying potential 'weak spots' or commonly targeted aspects of your network and systems. Some of the more common vectors include:

#	Type	Description
1	External/removable media	An attack executed from a USB containing malware.
2	Attrition	A DDoS attack on a critical network or system.
3	Web	The redirection of web traffic to a malicious URL that installs malware on a victim's device.
4	Email	Phishing attacks that attempt to steal information and/or deploy malware to a victim's device.
5	Impersonation usage	For example, a domain that is created to imitate yours in an attempt to deceive victims (typically associated with phishing attacks).
6	Improper usage	Human error resulting in a breach of information security policy; or attack from a malicious insider resulting in a cyber security incident.

4. Roles and Responsibilities

The following section details the composition and functions of the <organisation> Incident Management Team (IMT) and the Senior Executive Management Team (SEMT).

4.1 Incident Management Team

The <organisation> IMT is responsible for managing responses to cyber incidents. The members of the <organisation> IMT are identified below.

Name	Contact Details	Title	IMT Role [suggested]
[Update as appropriate – the composition of your IMT will vary depending on the size of your organisation and available skills]		IT security manager [expand to include network engineers, system administrators etc]	**Incident manager** ▪ Planning and operations ▪ Intelligence and analysis ▪ Technical advice
		Organisation security manager	▪ Investigation (if suspected internal threat) ▪ Law enforcement liaison
		Business continuity advisor*	▪ Facilities support ▪ Business and community consequence analysis / management
		Communications, engagement and media advisor*	▪ Information and warnings ▪ Internal communications ▪ Media and community Liaison
		Legal advisor*	▪ Legal advisory services (incl. regulatory compliance)
		Finance and procurement advisor*	▪ Facilities and finance support
		Administration and record keeping*	▪ Administration support, incl Incident Log, Evidence and Situation Reporting
[Include details of any 3rd party vendors that support systems/applications]		Lead contact for <system/application>	▪ System/application support
Victorian Government Cyber Incident Response Service	1300 CSU VIC (24/7) cybersecurity@dpc.vic.gov.au	Incident response and coordination services; Emergency Management	▪ Technical/forensic investigations and communications support
AusCERT – cyber technical advisory services	1800 723 009 (24/7) vicsoc@auscert.org.au	Incident analysis, containment, eradication and recovery advice	▪ Technical investigations and support

*denotes an optional IMT position that may be activated only if required, based on the circumstances of an incident.

4.1.1 The Senior Executive Management Team

More serious cyber incidents may require the formation of the <organisation> SEMT. The SEMT may form at the request of the Incident Manager, or at the discretion of the <organisation> Chief Executive Officer [or Chief Information / Security Officer, if more appropriate].

The SEMT should provide strategic oversight, direction and support to the IMT, with a focus on:

- Strategic issues identification and management
- Stakeholder engagement and communications (including ministerial liaison, if appropriate)
- Resource and capability demand (including urgent logistics or finance requirements, and human resources considerations during response effort).

If a SEMT is not able to form, ensure that someone else in the organisation has the delegation to make critical decisions.

Name	Contact Details	Title	SEMT Role [suggested]
[Update as appropriate]		Chief Executive Officer	▪ SEMT Chair
		Chief Information Officer	▪ SEMT Deputy Chair
		Chief Information Security Officer	▪ SEMT Deputy
		Finance / Procurement	▪ Emergency procurement and expenditure oversight
		Legal	▪ Regulatory compliance; cyber insurance
		Communications and stakeholder engagement	▪ Public relations and stakeholder engagement
		People and culture	▪ Staff welfare management

5. Incident Response Process

For assistance responding to cyber incidents contact the Victorian Government Cyber Incident Response Service on 1300 CSU VIC (24/7) or cybersecurity@dpc.vic.gov.au (business hours).

Quick Reference Checklist of Incident Response Actions

#	Activity
1	Conduct analysis to determine whether an incident has occurred / or is occurring
2	Determine the scope, impact and severity of the incident; categorise the incident
3	Activate your IMT (and SEMT, if appropriate) to manage the response effort; begin documenting the situation
4	Develop and implement a resolution action plan detailing containment, eradication and recovery activities; gather and record evidence
5	Identity affected stakeholders – who will be impacted by the incident?
6	Develop a notifications strategy and communicate key messages with affected stakeholders
7	Confirm the threat has been eradicated and return affected systems/services to normal function (test systems/services to confirm expected functionality)
8	Stand down your IMT/SEMT (when authorised by appropriate delegate); determine any stakeholder communications requirements
9	Conduct a post incident review to identify things that worked well and any opportunities for improvement; document your learnings/insights
10	Update your incident response plan to include any key learnings/insights

Step 1: Detection and Analysis

5.1.1 Incident Detection

There is no single process for detecting a cyber incident. Detection often involves:

- **Precursors:** detecting that a cyber-attack might occur in the future, such as the receipt of a threatening email or news of a global malware/ransomware attack (note: this form of detection is rare).
- **Indicators**: detection that an incident may have occurred (e.g. intrusion detection alerts, file names with odd characters, configuration changes).
- **Security Monitoring:** Referral from a managed security service provider or another organisation/stakeholder, alerting to the presence of a cyber incident.

The table below provides some common indicators that suggest you might be experiencing a cyber security incident.

Indicators	Examples
Reports of unusual or suspicious activity by staff or external stakeholders.	A staff member receives an email asking them to confirm their network credentials or to provide other personal or sensitive information.
	Multiple staff report being 'locked out' of their network accounts.
	An external stakeholder reports receiving spam or phishing emails from your organisation.
	A member of the public approaches your organisation to report the discovery (or exploitation) of a security vulnerability.
System(s)/service(s) not operating or functioning as expected	For example, one or more IT systems or services may cease functioning, or may not function as expected, and there is not a readily identifiable cause (such as a planned upgrade or outage).
	SSL Certificates broken; for example customers complaining that your organisation's website has a broken link.
Unusual Activity	Network administrators observe a large number of 'bounced' emails containing suspicious or unexpected content; or there is a substantial change in network traffic flows with no readily identifiable cause.
	Network or application logs show multiple failed login attempts from unfamiliar remote systems, such as overseas locations.
	Anti-virus alerts – a notification from your anti-virus service or a managed service provider that it has detected suspicious activity or files on your network, which require analysis and remediation.
	Service or admin accounts modifying permissions; admin accounts adding standard users to groups; service accounts logging into a workstation.
	A system administrator observes a filename with unusual characters, or expected files are no longer visible on the network.

5.1.2 Incident Analysis

After considering the indicators of a potential cyber incident, it is important to confirm whether an incident has, or continues, to occur. The following table identifies steps that are useful in confirming the presence of a cyber incident.

Action	Description
Updated Resources	Ensure you have access to the latest: - Network diagrams - IP addressing schemas - Port lists - Documentation that may include system designs/architecture, security plans, GPO configuration, etc.
Reviewing log entries and security alerts	Are there any unusual entries or signs of suspicious behavior on the network or applications?
Have Standard Operating Procedures (SOPs) for different operating systems	For Windows workstations, follow a SOP on what to look for or review (i.e. specific event log sources, the types of events to search for, etc.). The same applies for Linux and Unix Operating Systems.
Consult with network and application experts	Is there a legitimate explanation for the unusual or suspicious activity that has been observed?
Conduct research	Research and review any open source materials (including via internet search engines) relating to the unusual or suspicious activity that is observed (for example, consider performing a search on any unusual filenames that are observed on the network).
Watch list / monitor list	Develop a list where suspected accounts or IPs can be added to monitor their ongoing activity.
IMPORTANT	Do not 'ping' or try to communicate with a suspected IP address or URL from your own network, as you may tip off the attacker that you have detected their activity. This should be conducted by a third party that is able to conduct this activity securely and anonymously.

It is important to consider the timeliness of your analysis. Lengthy analysis is useful for developing a comprehensive understanding of an incident but can also impede the overall response process.

Generally, it is advisable to spend up to one hour on the initial incident analysis phase before seeking outside assistance.

5.1.3 Incident Classification

The following table provides a guide for classifying the category of a cyber incident. The table also provides indicators to consider when determining whether a cyber incident is increasing or decreasing in impact and severity.

Category	Description	Trigger(s) for escalation
Cyber Event	A suspected (or unconfirmed) cyber incident, with no observable impact to systems or services.	Substantial increase in cyber security alerts; or continued cyber security alerts with potential to breach security controls. Confirmed breach of security controls.
Cyber Incident	Successful compromise of security controls that requires corrective action. Minor to moderate impact to services, information, assets, reputation or relationships. May form part of a national or international cyber incident.	Actual or high likelihood: • for major impact to services; or • to affect multiple organisations; or • data breach involving personal information.
Significant Cyber Incident	Successful compromise of security controls that requires corrective action. Major to significant impact to services, information, assets, government reputation, relationships and/or the community (but not an emergency situation). Any incident that involves: • more than one organisation; or • a data breach involving personal information.	A situation that: • has the potential to cause or is causing loss of life and extensive damage to property, infrastructure or the environment, or • Has the potential to have or is having significant adverse consequences for the Victorian community or a part of the Victorian community. **Immediately refer all significant cyber incidents and cyber emergencies to the Victorian Government Cyber Incident Response Service on 1300 CSU VIC (24/7).** **The Victorian Government Cyber Incident Response Service supports the Department of Premier and Cabinet as Victoria's control agency for cyber emergencies.** [IMPORTANT – Consider how you will align this document with your organisation's emergency management arrangements, if applicable]
Cyber Emergency	Successful compromise of security controls that: • has the potential to cause or is causing loss of life and extensive damage to property, infrastructure or the environment; or • has the potential to have or is having significant adverse consequences for the Victorian community or a part of the Victorian community; or • requires the involvement of two or more agencies to respond to the emergency.	

5.1.4 IMT Activation

If a cyber incident is confirmed and requires a team to manage the response effort, activate the IMT (note: some smaller incidents may be manageable without activation of the IMT).

The IMT should relocate to a dedicated operations room. The IMT operations room is located at <room details>. Contact <name and contact details> for after-hours access to the IMT operations room.

5.1.5 Incident Notifications

It is important to notify relevant stakeholders that a cyber incident has occurred or is occurring.

The scope, impact and severity of the incident should determine the extent of stakeholder notifications. More serious incidents will likely require engagement with a broader range of stakeholders.

Key stakeholders to notify include:

- [list relevant organisational senior executive and their contact details]
- [list relevant government departments or agencies (including regulators), based on your individual circumstances]
- [list relevant Ministerial Office contacts, if appropriate]
- The Victorian Government Cyber Incident Response Service – 1300 CSU VIC (24/7) (immediate notification required for significant cyber incidents and emergencies)
  - The Victorian Government Cyber Incident Response Service can liaise with Victoria Police and the Australian Cyber Security Centre on your behalf, if required.
  - Alternatively, if you are concerned that you have been a victim of cyber crime (including financial fraud), you may contact Victoria Police on ecrime@police.vic.gov.au or via the Australian Cybercrime Online Reporting Network at **https://www.acorn.gov.au**
- Your cyber insurance provider (if applicable)

The IMT, typically via the Incident Manager or communications lead, is responsible for managing these notifications on behalf of <organisation>.

[Consider developing a list or table that identifies the stakeholders relevant to each category of cyber incident]

5.1.6 IMT Documentation

Upon establishment, the IMT should immediately begin documenting information about the incident. This documentation includes 'situation updates' (Appendix A) and the 'incident log' (Appendix B).

Situation updates should contain the following information:

- Incident date and time (usually the date and time the incident was confirmed)
- The status of the incident – for example, new / in progress / resolved
- Incident type and classification – for example, malware / ransomware / DDoS etc.

- Scope – details of affected networks, systems and/or applications
- Impact – details of entities affected by the incident, and how they are affected
- Severity – details of the impact of the incident on the organisation(s) (for example, what business services are impacted?)
- Contact details for the incident manager and key IMT personnel.

Situation updates should be prepared and disseminated to <organisation> internal stakeholders at regular intervals. It is important to be proactive with the development and dissemination of your situation reports, to reduce the need for stakeholders to approach you with various questions about the incident.

The incident log should be maintained by a member of the IMT (or a delegate). The incident log should capture minutes from each IMT meeting, details of all critical decisions (including the rationale for a decision), operational actions taken, action items and future meeting dates and times. Each entry to the incident log should include date, time and author details.

Step 2: Containment and Eradication

5.1.7 Resolution Action Plan

The IMT should develop a **Resolution Action Plan** (**Appendix C**) for resolving the incident.

The Resolution Action Plan should consider the immediate and future steps required for containing the incident and eradicating any threats that might exist; and the future steps required for restoring systems and services. The the Resolution Action Plan should be reviewed throughout the process as it may change depending on what evidence is acquired during the detection and analysis steps.

The key elements of the Resolution Action Plan are:

- **Containment actions** – what are you doing now to contain and the incident/threat and prevent the spread of the situation?
- **Eradication actions** – what are you doing to remove the incident/threat from your environment?
- **Capability and capacity requirements** – what resources do you require for the plan to be successful?
- **Communications actions** – what messages are you communicating, to whom, when and how?

The details of the Resolution Action Plan will vary depending on the type of incident that you experience. There is no 'one size fits all' approach.

When developing the Resolution Action Plan, it is important to consider:

- How long will it take to resolve the incident?
- What resources are required to resolve the incident (if not already included in the IMT)?
- What systems/services will be affected during the resolution process? What services are impacted?

5.1.8 Evidence Preservation

The IMT will collect and record evidence about the cyber incident to support detailed forensic investigations, including law enforcement efforts to identify and prosecute potential cyber-attackers.

To the best of its ability, and where relevant to the incident, the IMT should collect and record the following evidence:

- 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.

When gathering evidence, it is important to consider the following steps:

- Nominate a member of the IMT to be responsible for collating, recording and storing all evidence that is collected.
- The IMT will create and maintain a log of all evidence collected, detailing the date and time evidence was collected, who it was collected by, and details of each item collected. See **Appendix D** for a template to use for this task.
- Ensure that all evidence is securely stored and handled only by the nominated IMT member, with limited access provided to other staff.
- Any access to evidence should be clearly recorded in the evidence log, including the rationale for access. This is important in maintaining the 'chain of custody' for collected evidence.
- Minimise the number of times evidence is transferred between staff. Record details of any evidence transfer between staff.

Step 3: Communications and Engagement

5.1.9 Internal Communications

Beyond the regular situation reports, it may be necessary to brief employees of your organisation about a cyber incident. This is important if organisational IT networks, systems or applications no longer operate as expected, or if the situation has potential to generate media or public interest.

Key messages to consider when communicating with employees include:

- What happened and why did it happen?
- What will happen in the immediate future?
- What are employees expected to do?
- Who can employees contact if they have questions?

All internal communications must be reviewed and approved by <communications lead and the Incident Manager> prior to release.

5.1.10 External Communications

Depending on the impact and severity of a cyber incident, it may be necessary to communicate with external stakeholders (including ministers, media and the public). This is particularly important if the incident affects IT networks, systems or applications relied upon by third-parties, such as public facing websites or services.

Key messages to consider when communicating with external stakeholders include:

- What happened and why did it happen?
- What systems/services are affected?
- What steps are being taken to resolve the situation?
- Is it possible to say when the situation will be resolved?
- What are external stakeholders expected to do?
- Who can external stakeholders contact if they have questions/concerns?

All external communications must be reviewed and approved by <communications lead and the Incident Manager> prior to release. If the SEMT is activated, the SEMT Chair should approve all external communications prior to release.

Step 4: Recover

The IMT should develop a plan for recovering from the cyber incident.

The recovery plan should detail the approach to recovering IT networks, systems and applications once containment and eradication is complete. Depending on the type and severity of an incident, the IMT may need to develop this plan in conjunction with business continuity and IT services advisors.

The recovery plan should include the following elements:

- a plan to restore systems to normal operation
- a process of continual monitoring to confirm that the affected systems are functioning normally
- a plan (if applicable) to remediate vulnerabilities to prevent similar incidents.

It is important to consider that, in some circumstances, a recovery plan may include the finalisation of a related criminal investigation (including forensic evidence collection), which may need to occur before recovery is possible.

5.1.11 Stand Down

Following the implementation and execution of an agreed recovery plan, the Incident Manager should advise the IMT that it is acceptable to stand down.

If the SEMT is activated, only the SEMT Chair (or Deputy Chair) should issue stand down instructions, following consultation with the Incident Manager.

The Incident Manager should gather copies of all notes taken during the response effort to assist with a Post Incident Review.

Step 5: Learn and Improve

This step is one of the most important phases in the incident response process, and the one that is most often overlooked. Learning from each incident enables the IMT to continually improve its processes and procedures for managing cyber incidents.

The IMT (and SEMT, if activated) should come together for a Post Incident Review to discuss:

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organisations have been improved?
- What corrective actions can prevent similar incidents in the future?

- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyse, and mitigate future incidents?

The discussion should be documented and any key insights / lessons learnt shared with all parties involved. Any recommendations to arise from the discussion should be documented in a corresponding action plan that states how the recommendation will be actioned, by whom and when.

5.1.12 Update Incident Response Plan

This plan will be continually updated to reflect better practice in cyber incident response activities, including following any relevant post incident reviews.

Appendix A. **Situation update** (template)

DATE OF ENTRY:	**TIME OF ENTRY:**	**AUTHOR:**
DATE AND TIME INCIDENT DETECTED		
CURRENT STATUS	New / In Progress / Resolved	
INCIDENT TYPE		
INCIDENT CLASSIFICATION	Incident / Significant Incident / Emergency	
SCOPE – list the affected affected networks, systems and/or applications; highlight any change to scope since the previous log entry		
IMPACT – list the affected stakeholder(s); highlight any change in impact since the previous log entry		
SEVERITY – outline the impact of the incident on the stakeholder(s); highlight any change to severity since the previous log entry		
NOTIICATIONS ACTIONED/PENDING		
ADDITIONAL NOTES		
CONTACT DETAILS FOR INCIDENT MANAGER		
DATE AND TIME OF NEXT UPDATE		

Appendix B. **Incident Log** (template)

DATE / TIME	NOTES (log, Record facts, decisions and rationale)
Start time	Start of Incident

Appendix C. **Resolution action plan** (template)

DATE AND TIME	**CATEGORY** (Contain / Eradicate / Recover / Communications)	**ACTION**	**ACTION OWNER**	**STATUS** (Unallocated / In Progress / Closed)

Appendix D. **Evidence register** (template)

DATE, TIME AND LOCATION OF COLLECTION	**COLLECTED BY** (name, title, contact and phone number)	**ITEM DETAILS** (quantity, serial number, model number, hostname, media access control (mac) address, and ip addresses)	**STORAGE LOCATION AND LABEL NUMBER**	**ACCESS –** date, time, person and rationale for access after collection

Appendix E. Assets and key contacts (template)

SITE INFORMATION

IP SUBNET	
DHCP SCOPE	
CORE ROUTER IP	
DNS SERVERS (INTERNAL) / LOGS & LOCATIONS	
DNS NAME / LOGS & LOCATION	
SECONDARY DNS NAME (EXTERNAL)	

INTERNET CONNECTION / COMMUNICATIONS

INTERNET SERVICE PROVIDERS IP & CONNECTION DETAILS	
NETWORK PROVIDER IP & CONNECTION DETAILS	
VOIP / PABX PHONE SYSTEM DETAILS IPs & NUMBER RANGE	
FIXED LINE SERVICES & HARDWARE	
3G/4G MOBILE DATA SERVICES & HARDWARE	
SATELLITE PHONE SERVICES & HARDWARE	
SINGLE POINT OF FAILURE ANALYSIS – COMMUNICATIONS INFRASTRUCTURE	

FIREWALL & SECURITY

FIREWALL SOFTWARE / HARDWARE	
WIRED NETWORK	
WIRELESS NETWORK	
SINGLE POINT OF FAILURE – FIREWALL INFRASTRUCTURE	

SITE REMOTE ACCESS

REMOTE ACCESS METHODS / LOGS & LOCATIONS	
SINGLE POINT OF FAILURE ANALYSIS – REMOTE ACCESS INFRASTRUCTURE	

WIRED NETWORK SWITCH INFRASTRUCTURE

HARDWARE / FIRMWARE / LOGS & LOCATIONS	
SINGLE POINT OF FAILURE ANALYSIS	

WIRELESS NETWORK SWITCH INFRASTRUCTURE

HARDWARE / FIRMWARE / LOGS & LOCATIONS	
SINGLE POINT OF FAILURE ANALYSIS	

INDUSTRIAL CONTROL SYSTEMS / SCADA INFRASTRUCTURE

SCADA PLC RTU HARDWARE / FIRMWARE / LOGS & LOCATIONS	
AUTHENTICATION METHODS & CONTROLS	
FUNCTIONAL ANALYSIS	
PROCESS FLOW DIAGRAM	
CONFIGURATION BACKUP SCHEDULE / LOCATIONS	
ALERT / ALARM SYSTEMS & THRESHOLDS	
SINGLE POINT OF FAILURE ANALYSIS	

DATA BACKUP

BACKUP SOFTWARE	
BACKUP LOCATION & RESTORATION TIMEFRAMES	
DATA RETENTION REQUIREMENTS	

DISASTER RECOVERY PLAN

IDENTIFIED HIGH AVAILABILITY? (YES / NO)	
REQUIRED UP TIME (%)	
REQUIRED RETURN TO OPERATION (Hrs)	

REDUNDANT POWER SUPPLY / UPS INFRASTRUCTURE

UPS HARDWARE / LOCATION	
BATTERY CAPACITY / RUN TIME	
CONNECTED DEVICES	

REDUNDANT POWER SUPPLY / GENERATOR INFRASTRUCTURE

GENERATOR HARDWARE / LOCATION	
FIXED OR PORTABLE	
CAPACITY (KVA)	
FUEL TYPE / CAPACITY (L)	
FUEL CONSUMPTION (L/Hr)	
ON SITE FUEL STORAGE (L) & LOCATIONS	
FUEL SUPPLY ARRANGEMENTS / AGREEMENTS	
DOCUMENTED FAIL OVER / RESTORATION OF SERVICES.	

ADMINISTRATION SYSTEMS (Supporting ICT systems)

WEB PROXY SERVER DETAILS / LOGS & LOCATIONS	
DOMAIN CONTROLLER DETAILS / LOGS & LOCATIONS	
WEB SERVER DETAILS / LOGS & LOCATIONS	
SERVER ENVIRONMENT OPERATING SYSTEM DETAILS / LOGS & LOCATIONS	
VIRTUAL SERVER HOST ENVIRONMENT DETAILS / LOGS & LOCATIONS	

EMAIL SYSTEMS

EMAIL SERVER DETAILS / LOGS & LOCATIONS	

DATABASE SYSTEMS

SERVER DETAILS / LOGS & LOCATIONS	
PRODUCTION DATABASE DETAILS / LOGS & LOCATIONS	
TEST DATABASE DETAILS / LOGS & LOCATIONS	

CLOUD SERVICE PROVIDERS

HOSTED SERVICE PROVIDERS & SLAs	

STAFF DESKTOP / LAPTOP / TABLET SYSTEMS

CLIENT ENVIRONMENT OS / LOGS & LOCATIONS	
CLIENT HARDWARE MANUFACTURER / MODEL	