MALWARE INCIDENT PREPARATION AND RECOVERY GUIDE

Prepared By:

National Data Management Authority
March 2023

Document Status Sheet

	Signature	Date
Policy Coordinator (Cybersecurity)	**Muriana McPherson**	**31-03-2023**
General Manager (NDMA)	**Christopher Deen**	**31-03-2023**

Document History and Version Control

Date	Version	Description	Authorised By	Approved By
31-03-2023	**1.0**		**General Manager, NDMA**	**National ICT Advisor**

Summary

1. This Guide define recommended activities to adequately prepare for, detect, analyse, and remediate (contain, eradicate, and recover), malware incidents.
2. It was adapted from NCC Group Cyber Incident Response Malware Playbook
3. This is a living document which will be updated annually or as required.
4. Submit all inquiries and requests for future enhancements to the Policy Coordinator, NDMA.

1.0 Purpose

The purpose of this guide is to define recommended activities that should be implemented to help Public Sector Organisations to adequately prepare for, detect, analyse, and remediate (contain, eradicate, and recover), malware incidents. The guide also identifies the key stakeholders that are required to undertake specific activities.

2.0 Authority

The Permanent Secretary, Administrative Head, Head of Human Resources or their designated representative of the Public Sector Organisation is responsible for the implementation of this policy. For further information regarding the foregoing, please contact the Policy Coordinator - National Data Management Authority (NDMA).

3.0 Scope

These guidelines encompass all good practices that the Government of Guyana ICT personnel must implement to ensure adequate preparation and recovery from malware incidents.

4.0 Information Statement

When a cyber-attack occurs, an organisation must respond to control the impact on the organisation's critical services and infrastructure, reputation, customers, and employees. A cyber-attack can be described as the deliberate exploitation of computer systems, technology-dependent enterprises, and networks[1]. Cyber-attacks use malicious code to alter computer code, logic, or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft[1]. With those few vivid thoughts in mind, this document will serve as a guideline to help agencies better prepare for and recover from malware incidents.

According to Microsoft, "Malware" is short for malicious software and is typically used as a catch-all term to refer to any software designed to cause damage to a single computer, server, or computer network[2]. Malware can include computer viruses, worms, trojan horses, spyware, rootkits, botnet software, keystroke loggers, ransomware, adware, and malicious mobile code. Sophisticated malware such as ransomware is used by script kiddies, neophytes, and skilled hackers to carryout vicious cyber-attacks on organizations.

[1] https://www.techopedia.com/definition/24748/cyberattack

[2] https://docs.microsoft.com/en-us/previous-versions/tn-archive/dd632948(v=technet.10)?redirectedfrom=MSDN

5.0 Guideline

(1)Preparation Phase

Preparation Phase	
Phase objectives	The preparation phase has the following objectives: ✓ Prepare to respond to cyber security incidents in a timely and effective manner. ✓ Prepare organizational assets for malware outbreak. ✓ Inform employees of their role in remediating a malware incident including reporting mechanisms.

Activity	Description	Stakeholders
Resource Provisioning	1. Review the adequacy of resources to properly monitor and defend the organisation against cyber-attacks. This may include hiring additional workers, training existing employees, and providing the requisite hardware and software tools to support their efforts. 2. Critical to this effort is to ensure adequate budgetary allocation is made for the acquisition of licensed software for organisational use	✓ Administrative Head of Ministry / Head of Agency ✓ Head of Human Resources ✓ Head of Information Technology (IT)
Prepare to Respond	Activities may include, but are not limited to: 1. Create an **inventory** and keep track of all computing assets: (i) hardware devices connected to the organisation's network and (ii) software applications installed on devices. Note: This would make it easier to detect rouge systems and unauthorised software on your network. 2. Ensure that all desktop/laptop and server systems used to carry our work for the organisation have authentic **licensed software** installed. This include both operating system (for example Microsoft Windows) and application software (for example Microsoft Word and Excel).	✓ Head of Information Technology (IT) ✓ Network Security Administrator ✓ Information Security Administrator ✓ Administrative Head of

Activity	Description	Stakeholders
	Note: The presence of unlicensed or "cracked" software presents a ripe environment for malware to infiltrate computer systems. 3. Ensure that all Desktops/Laptops/Servers/Network Devices and software are **securely configured**. Note: Devices delivered from manufacturers and resellers usually contain open services and ports, default accounts and passwords, and pre-configured settings which can be exploited by attackers if left in their default state and therefore must be adjusted. 4. Ensure that all software installed on desktop/laptop/servers and network devices receive vendor supplied **software updates and patches** on a monthly or more frequent basis and that such updates are tested prior to deployment. Note: This would ensure that computer systems are protected against known vulnerabilities. 5. Ensure that all desktop/laptop and server systems have a **licensed anti-malware** solution deployed and that it is configured to receive daily vendor updates and to automatically scan systems for the presence of malware. Note: This would ensure that computer systems are protected against known malware. 6. Ensure that sensitive and critical organisational data is properly identified and that **daily backups** are created and stored in a separate, protected offline location. Of note, critical data located on user computers/laptops must also be backed up. It is important to test the ability to recover data from backups at least quarterly. Note: This would ensure that in the event of a ransomware attack, recent backup can be used to recover data. To ensure quick recovery of operations in the event of a cyber-attack, it is useful to create weekly image backup of critical servers. It is recommended that backup of data and images be retained for at least 90 days before archived. 7. Maintain and enforce **network-based URL filters**. Once correctly configured, and proactively managed, it could prevent malicious website traffic, and malware from infecting the organization's devices or accessing its data.	Ministry/ Head of Agency ✓ National Data Management Authority

Activity	Description	Stakeholders
	8. Ensure that **user accounts**, including administrative and service accounts are properly secured with the use of strong passwords and that all user accounts not in use are deleted or disabled. This includes deprovisioning user accounts for employees who have left the organisation. 9. Ensure that each user has a **unique login ID** and that access to devices/ applications/ data are assigned based on defined roles. This includes restricting administrative privileges to those whose roles requires this for example, to network/system administrators. 10. Ensure that the **network infrastructure** is well **documented**, kept current, and appropriate access to required documentation is available, including out-of-hours access, for the following: ○ Cyber Incident Response Plan (CIRP) ○ Network Architecture Diagrams ○ Data Flow Diagrams ○ Inventory of all Organisational Hardware Devices and Software assets 11. **Retain logs** from firewall and other network devices for not less than 90 days and make logs available upon request to support inspection and analysis in the event of cybersecurity incidents. Logs to retain include Dynamic Host Configuration Protocol (DHCP) and Network Address Translation (NAT) logs. Note: Log collection and analysis is critical for an organization's ability to detect malicious activity and respond to incidents quickly. **12.** Document and rehearse **cyber incident response procedures** and assign technical and business roles and responsibilities who will investigate and escalate incidents flagged with severity levels "critical" and "high" whose impact is "widespread" and "significant" to the organisation, to the National Data Management Authority Cybersecurity Incident Reporting System via the website: www.cirt.gy or via the telephone number listed on the website. Note: All actions taken at each stage must be documented. **See Appendix I for incident reporting guidelines.**	

Activity	Description	Stakeholders
Inform employees	Activities may include, but are not limited to: 1. Publish internal communications in line with the communications strategy to inform and educate employees on malware attacks and security awareness. 2. Conduct regular **security awareness training** to educate employees on how to interact with the organization's assets and data in a secure manner. Examples include: ○ How to recognise Phishing attacks and malicious emails. ○ How to create strong passwords and credential management. ○ How to recognise and report a suspected cyber incident 3. Ensure regular security training is mandated for those employees managing personal, confidential, or high-risk data and systems. This includes training for your Information Technology (IT) employees.	✓ Head of Information Technology (IT) ✓ Head of Human Resources ✓ National Data Management Authority

(2)Detection Phase

Detection Phase
The detection phase has the following objectives: ✓ Detect and report a breach or compromise of the confidentiality, integrity, or availability (CIA) of organizational data. ✓ Complete initial investigation of the malware. ✓ Report the malware formally to the correct teams (e.g., GNCIRT) as a cyber incident.

Activity	Description	Stakeholders
Detect and report the incident	Activities may include, but are not limited to: 1. Use an active discovery tool to detect and generate an alarm when a new device is connected to the organisation's network. This is useful in detecting rouge devices which may introduce vulnerability to the network. 2. Use an active discovery tool to detect and generate an alarm when an unauthorised software is installed on the network.	✓ Head of Information Technology (IT) ✓ Network Security Administrator ✓ Information Security Administrator

Activity	Description	Stakeholders
	3. Use a centralised tool to monitor and detect the software update and patch status of devices on the network. This is useful for identifying systems that do not have the latest software update and patches installed. 4. Use a centralised anti-malware solution to monitor and generate an alarm when a virus is detected on a device and when devices are missing critical anti-malware updates. 5. Deploy a centralised security event and alerting system such as a security incident and event management (SIEM) solution which includes vendor defined correlation alerts, log analysis, and intrusion detection mechanism. Configure it to receive logs from all network devices and generate an alarm of any indicator of compromise. 6. **Assign responsible personnel** to receive alarms from the tools outlined above.	✓ National Data Management Authority Incident Response Team
Initial investigation of the incident	**1. Assign responsible personnel** to complete initial investigations. Note: Isolated malware infections are to be expected from time to time and will usually be resolved automatically by the anti-malware technology implemented by the organization along with the assigned organisational personnel. **2.** Collate initial incident data including as a minimum for the following. ○ A timeline of when the malware was first detected, and other significant events. ○ Whether the malware was detected by the anti-malware solution or identified through other means. ○ The probable scope of the infection, in terms of the systems and/or applications affected. ○ Whether the malware appears to be spreading across the infrastructure. ○ The probable nature of the malware infection, if known. ○ Whether the anti-malware solution has successfully quarantined/cleansed the infection. ○ Likely containment options (e.g., on the basis of publicly available information, for known malware).	✓ Head of Information Technology (IT) ✓ Network Security Administrator ✓ Information Security Administrator ✓ National Data Management Authority Incident Response Team

Activity	Description	Stakeholders
	3. Review the cyber incident categorisation to validate the cyber security incident type as a malware attack and assess the incident severity and impact, based upon the initial investigation.	
Incident Reporting	**1.** Incidents, usually flagged with "medium" or "low" severity must be documented and included in half-yearly compliance reports to the National Data Management Authority Cybersecurity Incident Reporting System in accordance with Department of Public Service circular 1/2019 dated 1st April 2019. **See Appendix II for a copy of the circular.** **2.** Incidents flagged with severity levels "critical" and "high" whose impact is "widespread" and "significant" to the organisation must be reported **within** 72 hours of discovery to the National Data Management Authority Cybersecurity Incident Reporting System. **See Appendix I for incident reporting guidelines.** This document includes the definitions of incident severity and impact (incident prioritisation) and incident classification.	✓ Head of Information Technology (IT) ✓ National Data Management Authority Incident Response Team

(3)Analysis Phase

Analysis Phase
The analysis phase has the following key objectives: ✓ Analyze the cyber incident to uncover the scope of the attack. ✓ Identify and report potentially compromised data and the impact of such a compromise. ✓ Establish the requirement for a full forensic investigation. ✓ Develop a remediation plan based upon the scope and details of the cyber incident.

Activity	Description	Stakeholders
Analyse the extent of the incident	Activities may include, but are not limited to: 1. Activate the organisation's cyber incident response procedures. 2. Engage technical staff and NDMA's incident response team depending on the severity and impact of the incident. 3. Fine tune the scope of the attack ○ A timeline of when the malware was first detected, and other significant events.	✓ Head of Information Technology (IT) ✓ Network Security Administrator

Activity	Description	Stakeholders
	○ Whether the malware was detected by the anti-malware solution or identified through other means. ○ Possible means of entry. ○ The probable scope of the infection, in terms of the systems and/or applications affected. ○ Whether the malware appears to be spreading across the infrastructure. ○ Determine whether the malware appears to be attempting to communicate with outside parties. ○ The probable nature of the malware infection, if known. ○ Whether the anti-malware solution has successfully quarantined/cleansed the infection. ○ Likely containment options (e.g. on the basis of publicly-available information, for known malware). 4. Classify the malware to determine the family it belongs to. 5. Review affected infrastructure and logs for indicators of compromise to identify any additional compromised system(s). 6. Examine threat intelligence feeds to determine if the malware attack is bespoke and targeted at specific accounts, infrastructure, or systems. 7. Verify all infected assets are in the process of being quarantined.	✓ Information Security Administrator ✓ National Data Management Authority Incident Response Team

(4)Remediation – Contain, Eradicate and Recover

Remediation Phase
The remediation phase has the following objectives: ✓ Contain the effects of the malware on the targeted systems. ✓ Eradicate the malware from the network through agreed mitigation measures. ✓ Recover affected systems and services back to a Business as Usual (BAU) state.

Activity	Description	Stakeholders
Containment	Contain the technical mechanisms of the malware attack. Of note: the actual containment procedure would be based on the type of malware/incident detected. Some containment actions include:	✓ Head of Information Technology (IT)

Activity	Description	Stakeholders
	1. Identify the infected device(s) and physically disconnect them from the network. Business continuity options for users affected by such disconnection include: a. Replacing disconnected devices with fresh installation or backup images. Ensure they have the relevant updates and secure configuration prior to deployment (see Preparation Phase) b. Directing users whose devices are disconnected to work from an alternative location, such as another office, a Disaster Recovery facility or from home. 2. Monitor for any new infections which might suggest that the malware is spreading across the infrastructure and alert NDMA Incident Response Team of any significant changes in the scope of the incident (e.g., the infection of a previously unaffected business system or site). 3. Ensure that the latest malware definitions have been deployed across the anti-malware solution 4. Initiate an organization wide anti-malware scan. 5. Where necessary the organisation's disaster recovery process should be followed. 6. Suspend the login credentials of suspected compromised accounts 7. Inform business data owner(s) and stakeholders of the progress of containment activities.	✓ Network Security Administrator ✓ Information Security Administrator ✓ Administrative Head of Ministry / Head of Agency ✓ National Data Management Authority Incident Response Team
Eradication	Activities may include, but are not limited to: 1. Identify removal methods from the results of the malicious code analysis and trusted sources (AV providers). 2. Complete an automated or manual removal process to eradicate malware or compromised executables using appropriate tools. 3. Conduct a restoration of affected networked systems from a trusted back up.	✓ Head of Information Technology (IT) ✓ Network Security Administrator ✓ Information Security Administrator ✓ Administrative Head of

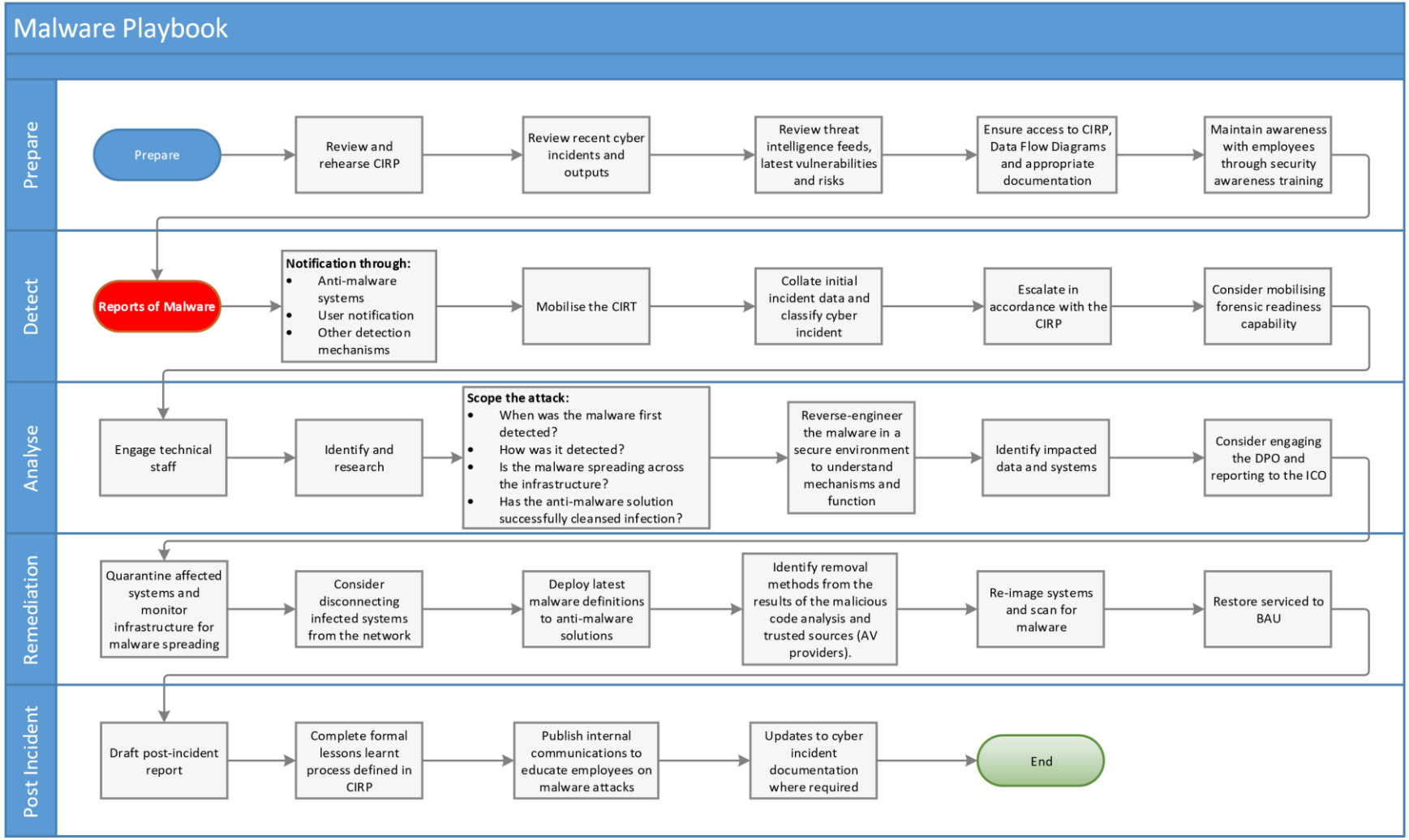
Activity	Description	Stakeholders
	4. Re-install any standalone systems from a clean operating system back-up before updating with trusted data back-ups. 5. Change any compromised account details. 6. Continue to monitor for signatures and other indicators of compromise to prevent the malware attack from re-emerging. 7. Confirm that all Desktops/Laptops/Servers/Network Devices and software back are in compliance with requirements 2 – 6 in the "Prepare to Respond" section of the Preparation Phase of this guide.	Ministry / Head of Agency ✓ National Data Management Authority Incident Response Team
Recover to Business as Usual (BAU)	Activities may include, but are not limited to: 1. Recover systems based on business impact analysis and business criticality. 2. Complete malware scanning of all systems, across the network infrastructure 3. Re-image systems. 4. Reset the credentials of all involved system(s) and users account details 5. Reintegrate previously compromised systems. 6. Restore any corrupted or destroyed data. 7. Restore any suspended services. 8. Establish monitoring to detect further suspicious activity. 9. Co-ordinate the implementation of any necessary patches or vulnerability remediation activities.	✓ Head of Information Technology (IT) ✓ Network Security Administrator ✓ Information Security Administrator ✓ Administrative Head of Ministry / Head of Agency ✓ National Data Management Authority

(5)Post Incident

Post-Incident Activities Phase
The post-incident phase has the following objectives: ✓ Complete an incident report including all incident details and activities. ✓ Complete the lessons identified and problem management process. ✓ Publish appropriate internal and external communications.

Activity	Description	Stakeholders
Incident Reporting	Activities may include, but are not limited to: Draft a post-incident report that includes the following details as a minimum: 1. Details of the cyber incident identified and remediated across the network to include timings, type, and location of incident as well as the effect on users. 2. Activities that were undertaken by relevant resolver groups, service providers and business stakeholders that enabled normal business operations to be resumed. 3. Recommendations where any aspects of people, process or technology could be improved across the organization to help prevent a similar cyber incident from reoccurring, as part of a formalized lessons identified process.	✓ Head of Information Technology (IT) ✓ Network Security Administrator ✓ Information Security Administrator ✓ Administrative Head of Ministry / Head of Agency ✓ National Data Management Authority
Lessons Identified & Problem Management	1. Complete the formal lessons identified process to feedback into future preparation activities. 2. Consider sharing lessons identified with the wider stakeholders. (This may include publishing external communications, if appropriate, in line with organisational communications strategy to provide advice to other agencies and inform press of the cyber incident). 3. Conduct root cause analysis to identify and remediate underlying vulnerabilities	✓ Head of Information Technology (IT) ✓ Network Security Administrator ✓ Information Security Administrator

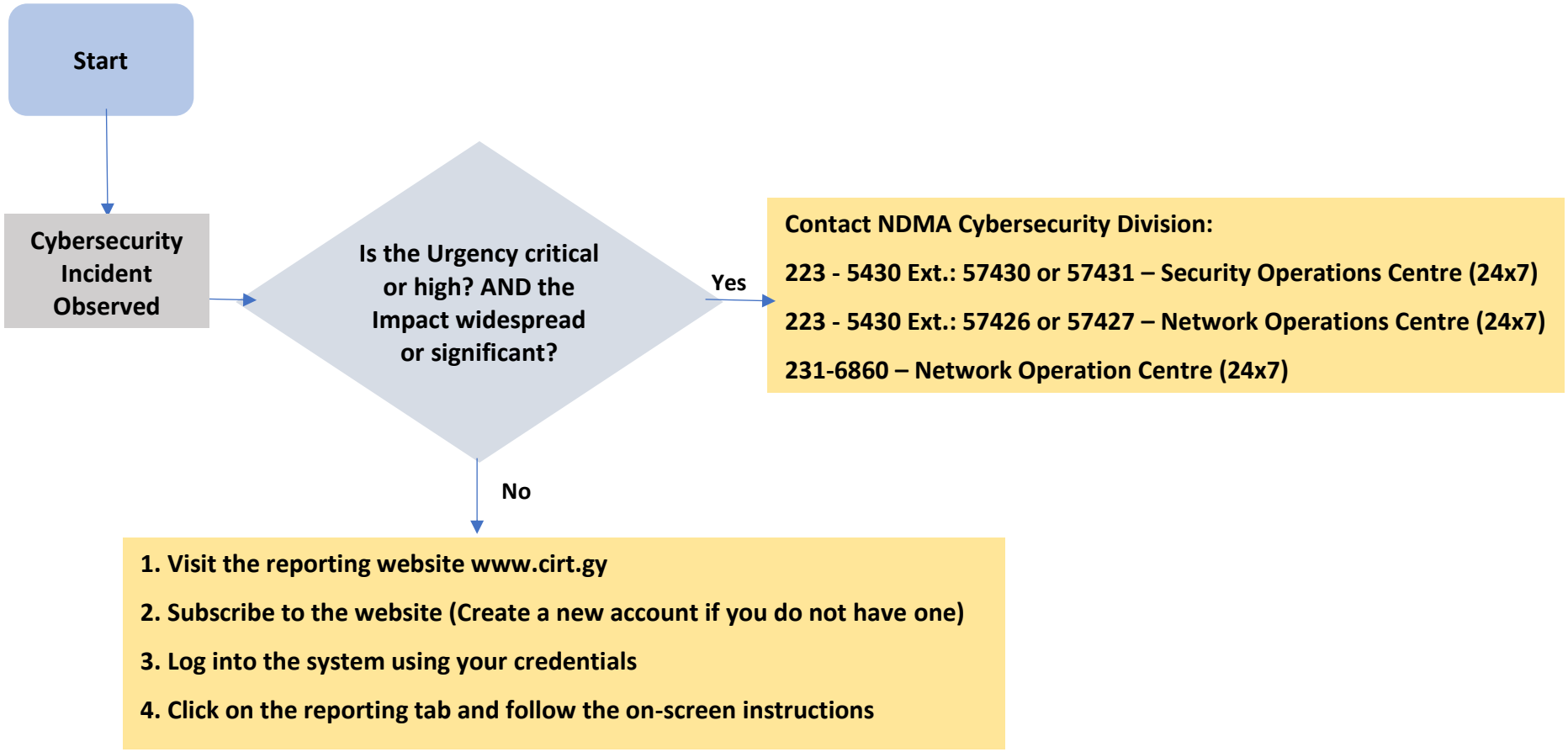
Flow Diagram[3]



[3] https://www.gov.scot/binaries/content/documents/govscot/publications/advice-and-guidance/2019/10/cyber-resilience-incident-management/documents/cyber-incident-response-malware-playbook/cyber-incident-response-malware-playbook/govscot%3Adocument/Cyber%2BCapability%2BToolkit%2B-%2BCyber%2BIncident%2BResponse%2B-%2BMalware%2BPlaybook%2Bv2.3.pdf

Appendix I: Incident Reporting Guidelines

Cybersecurity Incident Reporting Flow Diagram



How to Determine Incident Severity & Impact

- ✓ Report incidents flagged with urgency levels "critical" and "high" whose impact is "widespread" and "significant" immediately to the NDMA Cybersecurity Division **Security Operations Centre 24x7 telephone number: 223 - 5430 Ext.: 57430 or 57431**

- ✓ Report all other incidents **within** 72 hours of discovery to the National Data Management Authority Cybersecurity Incident Reporting System via the **www.cirt.gy website.**

- ✓ Incidents will be prioritised based on the urgency and impact of the incident relative to other government of Guyana Ministries/Agencies. The incident priority matrix outlined in Figure 1 below defines incident urgency and impact[4].

		Impact			
		Extensive/Widespread Enterprise, Region, or Segment	Significant/Large Business Unit, Department, Location	Moderate/Limited Few Users	Minor/Localized Single User
Urgency	Critical Can no longer work	1 - Critical	1 - Critical	2 - High	2 - High
	High Can no longer perform primary work functions	1 - Critical	2 - High	2 - High	2 - Medium
	Medium Work functions impaired	2 - High	3 - Medium	3 - Medium	3 - Medium
	Low Inconvenient	4 - Low	4 - Low	4 - Low	4 - Low

Figure 1: Incident Prioritisation

[4] https://www.concurrency.com/blog/june-2019/impact-urgency-matrix-defined

Incident Prioritisation Description

✓ Figure 2 below gives a detailed description of how incidents are prioritised.

Colour	Level	Severity	Description
Red	1	Critical	This level is reserved for severe or catastrophic cybersecurity incidents. Infrastructure may have been destroyed along with critical information system data. Incidents at this level may require the engagement of external stakeholders, such as the Police Force Cybercrime Unit. Incidents fall into this category for one of three reasons: 1. An entire segment is down, and no work functions can be carried out. 2. A department is down, and no work functions can be carried. 3. An entire segment of systems is down, and primary work functions cannot be carried out.
Gold	2	High	Major Disruption in Service Delivery. Incidents fall into this category for one of five reasons: 1. Few users can no longer perform work duties. 2. A user can no longer perform work duties. 3. A department is down, and primary work functions cannot be carried out. 4. Few users can no longer perform primary work duties. 5. An entire segment of government systems is down, and work functions are impaired.
Yellow	3	Medium	Minor Disruption in Service Delivery Incidents fall into this category for one of four reasons: 1. A user can no longer perform primary work duties. 2. A department is down, work functions are impaired. 3. Few users work functions are impaired. 4. A user within a Government Ministry or Agency work functions impaired.
Green	4	Low	Very Little or No Disruption in Service Delivery. This level represents typical, day-to-day operations. Attempts at infecting a non-critical information system may be occurring; however, endpoint controls such as a virus scanner prevents this from happening and removes the threat. If a non-critical system becomes infected, the organization's help desk can remove the threat and restore the system to normal operations.

Figure 2: Incident Prioritisation Description

Incident Classification

- ✓ Figure 3 below outlines the incident classification schema employed by the National Data Management Authority.

Classification[5]	Incident Type	Description
Ransomware	Ransomware	Ransom malware, or ransomware, is a type of malware that prevents users from accessing their system or personal files and demands ransom payment in order to regain access
Malicious Code	Malware, Virus, Worm, Trojan, Spyware, Rootkit	Software that is intentionally included or inserted in a system for a harmful purpose. A user interaction is normally necessary to activate the code.
Information Gathering	Scanning	Attacks that send requests to a system to discover weak points. This also includes some kind of testing processes to gather information about hosts, services and accounts. Examples: fingered, DNS querying, ICMP, SMTP (EXPN, RCPT, …), port scanning.
	Phishing	Masquerading as another entity in order to persuade the user to reveal a private credential.
Intrusion Attempts	Login attempts	Multiple login attempts (Guessing / cracking of passwords, brute force).
	Exploiting known vulnerabilities	An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardized identifier such as CVE name (e.g., buffer overflow, backdoor, cross site scripting, etc.).
	Exploiting unknown vulnerabilities	An attempt using an unknown exploit such as zero-day attack
Intrusions	Privileged account compromise	A successful compromise of a system or application (service). This can have been caused remotely by a known or new vulnerability, but also by an unauthorized local access. Also includes being part of a botnet.
	Unprivileged account compromise	
	Application compromise, Bot	
Availability	Denial of Service (DoS / DDoS)	By this kind of an attack a system is bombarded with so many packets that the operations are delayed or the system crashes. DoS examples are ICMP and SYN floods, Teardrop attacks and mail-bombing. DDoS often is based on DoS attacks originating from botnets, but also other scenarios exist like DNS Amplification attacks. However, the availability also can be affected by local actions (destruction, disruption of power supply, etc.) – or by Act of God, spontaneous failures or human error, without malice or gross neglect being involved.

Figure 3: Incident Classification

[5] Classification adapted from: https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy/

Appendix II – Incident Reporting Form

Incident Reporting Form

✓ Figure 4 below outlines the incident reporting form that must be filled when reporting an incident.

Name of Organisation: ……

Reported by: Name: ……

Designation: ……..

Contact Number: (preferably mobile) ……..

Date: ……

1. When, approximately, did the incident start? ……..
2. When was the incident detected? (Date and Time) ……
3. Please indicate the type of Incident (select all that apply)

□ Ransomware
□ Virus
□ Worm
□ Trojan
□ Phishing
□ Denial of Service
□ Distributed Denial of Service
□ Exploiting known vulnerabilities
□ Login attempts
□ Other, please state: …….

4. How was the incident detected?

□ Administrator/User
□ Anti-malware software
□ Security Information and Event Management Platform (SIEM)
□ Log review
□ Other, please state: ……..

5. What steps have been taken so far? Check all that applies.

□ No action taken
□ System disconnected from network
□ Updated virus definitions & scanned system
□ Sought external assistance
□ Restored backup from tape
□ Log files examined (saved & secured)
□ Incident reported to the police
□ Other, please state …….

6. Please state the impact of the incident (Please see Appendix 1 for guidance)

□ Critical
□ High
□ Medium
□ Low

7. Please state the estimated number of systems affected: …….

8. Please state the number of users affected ……

9. Any other comments:

   ……

   ……

   …….

   …….

10. Please attach all evidence of the incident (logs, email headers, screen shots)

Figure 4: Incident Reporting Form

Appendix III - What to Expect when NDMA Incident Response Team visits your Organisation.

What to Expect when the NDMA Incident Response Team visits your Organisation

✓ Figure 5 below the steps that will be taken by the incident response team when visiting an organisation.

Activity	Description	Stakeholders
Stakeholder's meeting	Activities may include but are not limited to the following: 1. Receive briefing on the incident at hand and actions that would have been taken so far by the organisation. 2. Define the scope and rules of engagement with the organisation. 3. Identify technical point of contacts for both teams during the analysis phase of the incident.	✓ Head of Information Technology (IT) ✓ Administrative Head of Ministry/ Head of Agency ✓ National Data Management Authority Incident Responders
Analysis of incident	1. Collect and review the information supplied on the incident reporting form (**see Appendix II**). If the form was not completed, then this must be completed by the identified point of contact. 2. Review applicable logs and relevant documentation depending on the nature and impact of incident. 4. Collect applicable screen capture of logs, malware messages and/or photographs of computer screens.	✓ National Data Management Authority Incident Responders ✓ Appointed technical point of contact(s)

Figure 5: Steps taken by NDMA Incident Response Team when visiting an organisation

6.0 Compliance

These guidelines shall take effect upon publication. Compliance is expected with all organisational guidelines, policies and standards. Failure to comply with the guidelines may, at the full discretion of the Permanent Secretary, Administrative Head, or Head of Human Resources of the Public Sector Organisation, may result in the suspension of any or all privileges and further action may be taken by the Ministry of Public Service.

7.0 Exceptions

Requests for exceptions to this guideline shall be reviewed by the Permanent Secretary, Administrative Head, Head of Human Resources of the Public Sector Organisation, or the Policy Coordinator, NDMA. Departments requesting exceptions shall provide written requests to the relevant personnel. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein.

8.0 Maintenance

The Policy Coordinator, NDMA shall be responsible for the maintenance of this guideline.

9.0 Contact Information

Submit all inquiries and requests for future enhancements to the Policy Coordinator, NDMA.

10.0 References

10.1 NCC Group: Cyber Incident Response Malware Playbook version 2.3. July 26, 2019

10.2 Centre for Internet Security: CIS Controls Version 8. May 2021