PremiumTrust Bank

Cyber Incident Response Plan

Classification: Internal

April 2023

Document Control Sheet

Version and Update History

Date	Document Version	Document Revision History	Document Author/Reviser
April 2023	1.0	Document creation	Musiliu Adeosun

Change Control

Change Clause/Frequency
The contents of this document are subject to change control on a twelve (12) months review cycle.

Contents

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 threats.

As the technology that underpins Information and Digital 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 perpetrating fraud, disrupting business or committing espionage.

This document supports PremiumTrust Bank in managing contemporary cyber threats and incidents. The application of this document will support PremiumTrust Bank 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 PremiumTrust Bank and coordinating response and resolution efforts to prevent or limit damage that may be caused.

1.3 Review

This incident response plan will be reviewed annually by Information & Cyber Security Group or following any cyber incident as deemed necessary by PremiumTrust Bank.

2. Terminology and Definitions

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

2.1 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 to):

1. Multiple failed sequential logons for a user
2. A user has disabled the antivirus on the computer
3. A user has deleted or modified system files
4. A user restarted a server

2.2 Cyber incident

A cyber incident occurs when there is a breach of explicit or implied information 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):

1. Denial of service attacks (DoS) that affect system or service availability
2. Virus or malware outbreak (including ransomware)
3. Compromise or disclosure of sensitive or personal information
4. Compromise of network credentials or an email account.
5. Unauthorized access
6. Other violations of PremiumTrust Bank IT Policies and Standards.

3. Common Cyber Incidents and Responses

The following is a list of cyber incident types, along with the minimum corresponding response activities required:

#	Type / Description	Initial response to minimize potential harm
1	Ransomware; a malicious software 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 device(s) 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 device.	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(s) while containment activities are confirmed, and eradication efforts are determined.
3	Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks; overwhelming an information and digital 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 unauthorized access.

5	Data breach; unauthorized access to sensitive or personally identifiable information.	Contain the data loss/spill as soon as possible. Alert Information & Cyber Security Group. 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 PremiumTrust Bank in identifying potential 'weak spots' or commonly targeted aspects of our 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	Web	The redirection of web traffic to a malicious website that installs malware on a victim's device.
3	Email	Phishing attacks that attempt to steal information and/or deploy malware to a victim's device.
4	Impersonation usage	For example, a domain that is created to imitate ours to deceive victims (typically associated with phishing attacks).
5	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. Common Cyber Incidents and Responses

The following section details the composition and functions of the PremiumTrust Bank Incident Management Team (IMT) and the Senior Executive Management Team (SEMT).

4.1 Incident Management Team (IMT)

An Incident Management Team (IMT) shall be established and approved by management. The PremiumTrust Bank IMT is responsible for managing responses to cyber incidents. The members of the PremiumTrust Bank IMT are identified below.

Name	Contact Details	Title	IMT Role
Musiliu Adeosun	M: 08099444234	Chief Information & Cyber Security Group	▪ Incident Manager ▪ Coordinate Cyber incident investigation
Weyinmi Otumara	M: 08037271798	Head, Information Technology Governance	▪ Coordinate Technology team and vendors supporting IT Infrastructure and applications
Kingsley Oriere	M: 08084857704	Chief Risk Officer	▪ Business continuity management
Adetayo Adejugbe	M: 08082960203	Group Head, Digital Banking	▪ Approve Action plans and communication content
Shina Atilola	M: 08182191489	ED Retail and Digital Business	▪ Internal communications ▪ External communications
Chukwuemeka Nwaogu	M: 08096511146	Company Secretary/Legal counsel	▪ Legal advisory services
Cosmas Uwaezuoke	M: 08055903344	Chief Compliance Officer	▪ Regulatory Compliance
Ayodele Shoyemi	M: 08025019937	Chief Finance Officer	▪ Finance support

4.1.1 The Senior Executive Management Team (SEMT)

More serious cyber incidents may require the formation of PremiumTrust Bank Senior Executive Management Team at the instance of the Chief Information & Cyber Security Groupr. 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
- Resource and capability demand (including urgent logistics or finance requirements, and human resources considerations during response effort).
- Ensure periodic, adequate and continuous training of the IMT team on how to respond, report cyber-incidents and conduct trend analysis to thwart future occurrence.

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

Name	Contact Details	Title	SEMT Role
Emmanuel Emefienim	M: 08059141298	Chief Executive Officer	▪ SEMT Chair The Managing Director shall be responsible for communication to the Board of Directors.
Cyril Osheku	M: 08023046639	Chief Operating Officer	▪ SEMT Deputy Chair
Shina Atilola	M: 08182191489	ED Retail & Digital Business	▪ Approve Action plans and communication content
Cosmas Uwaezuoke	M: 08055903344	Chief Compliance Officer	▪ Regulatory Compliance
Ayodele Shoyemi	M: 08025019937	Finance / Procurement	▪ Emergency procurement and expenditure oversight
Chukwuemeka Nwaogu	M: 08096511146	Legal	▪ Regulatory compliance
Fanen Acho	M: 08025097853	GH, Brand & Strategy	▪ Public relations and stakeholder engagement
Olanike Martins	M: 08023707807	Chief People Officer	▪ Staff welfare management

Musiliu Adeosun	M: 08099444234	Chief Information & Cyber Security Group	▪ Incident Manager

5. Incident Response Process

For assistance responding to cyber incidents, contact the Information & Cyber Security Group on infosec@premiumtrustbank.com

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; categorize the incident
3	Activate 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 IMT/SEMT (when authorized 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 incident response plan to include any key learnings/insights. Communicate key learning points to all staff. Update existing policy, procedural manuals and processes to prevent a re-occurrence.
11	Cybersecurity drill shall be performed annually. The cyber incident plan shall be reviewed periodically to ascertain its viability, effectiveness and efficiency.
12	All cyber-incidents (as defined in the CBN risk based cyber security framework), whether successful or unsuccessful, shall be reported, not later than 24 hours after such incident is detected, to the Director of Banking Supervision, Central Bank of Nigeria. Where necessary and

	applicable, additional information should be provided afterwards. This shall be reported by the Chief Information & Cyber Security Groupr.

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.
- Indicators: detection that an incident may have occurred (e.g. intrusion detection alerts, file names with odd characters, configuration changes).
- Security Monitoring: Detection of a cyber incident from information security monitoring activities of Security Operations Centre (SOC) team.

The table below provides some common indicators that a cyber security incident might be underway.

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 PremiumTrust Bank.
	A member of the public approaches the bank 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).
Unusual Activity	Network administrators observe many '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 the bank's anti-virus service or Security Operation Centre (SOC) team that it has

	detected suspicious activity or files on our network, which require analysis and remediation.
	Service or admin accounts modifying permissions; unauthorized use of 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, the Incident Management Team (IMT) shall confirm whether an incident has, or continues, to occur. The following table identifies steps that shall be used in confirming the presence of a cyber incident.

Action	Description
Updated Resources	The Incident Management Team (IMT) shall 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	Logs should be reviewed to ascertain whether there are any unusual entries or signs of suspicious behavior on the network or applications?
Consult with relevant third-party service provider	To determine if there is 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 the bank's network, as this may tip off the attackers.

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.
Cyber Incident	Successful compromise of security controls that requires corrective action. Minor to moderate impact to services, information, assets, reputation or relationships.	Actual or high likelihood: • for major impact to services; or • data breach involving personal information.
Significant Cyber Incident (Cyber crisis)	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). Any incident that involves: • more than one organization; or • a data breach involving personal information.	A situation that: • Has the potential to have or is having significant adverse consequences on the bank's service delivery capabilities.

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 or a war room. The IMT operations room is located at the head office Security Operations Centre on the 13th floor (short wing). Contact Musiliu Adeosun - 08099444234 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:

Internal Stakeholders:

- Board of directors
- Members of staff

External Stakeholders:

- Customers
- Public
- Regulators
- Law enforcement
- Shareholders
- Service providers
- Technical partners
- Industry fora to which the Bank is a member of

The underlisted national stakeholders if required by law

- National Identity Management Commission (NIMC)
- National Information Technology Development Agency (NITDA)
- Nigeria Computer Emergency Response Team (ngCERT)

The IMT, via the Chief Marketing Officer will be responsible for managing these notifications on behalf of PremiumTrust Bank.

5.1.6 IMT Documentation

In the event of a cyber incident and the activation of Incident Management Team, documentation of information about the incident should commence immediately. This documentation includes 'situation updates' (Appendix A) and the 'incident log' (Appendix B).

Situation updates should contain the following information:

1. Incident date and time (usually the date and time the incident was confirmed)
2. The status of the incident – for example, new / in progress / resolved
3. Incident type and classification – for example, malware / ransomware / DDoS etc.
4. Scope – details of affected networks, systems and/or applications
5. Impact – details of entities affected by the incident, and how they are affected
6. Severity – details of the impact of the incident on the bank (for example, what business services are impacted?)
7. Contact details for the incident manager and key IMT personnel.

Situation updates should be prepared and disseminated to PremiumTrust Bank's internal stakeholders at regular intervals. It is important to be proactive with the development and dissemination of situation reports, to reduce the need for stakeholders to approach IMT 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

A Resolution action plan (Appendix C) shall be developed by the IMT 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 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:

A. Containment actions – what actions are required now to contain the incident/threat and prevent the spread of the situation?

B. Eradication actions – what actions are required to remove the incident/threat from the bank's environment?

C. Capability and capacity requirements – what resources are required for the plan to be successful?

D. Communications actions – what messages are being communicated, to whom, when and how?

When developing the Resolution action plan for each cyber incident, the following shall be considered:

A. How long will it take to resolve the incident?

B. What resources are required to resolve the incident (if not already included in the IMT)?

C. 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:

1. Hard drive images and raw images
2. RAM images
3. IP addresses
4. Network packet captures and flows
5. Network diagrams
6. Log and configuration files
7. Databases
8. Investigation notes
9. Screenshots
10. Social media posts
11. CCTV, video and audio recordings
12. Documents detailing the monetary cost of remediation or loss of business activity.

When gathering evidence, the following steps shall be taken:

1. Nominate a member of the IMT to be responsible for collating, recording and storing all evidence that is collected.
2. 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. Appendix D shows the template to be used to collate data.

3. Ensure that all evidence is securely stored and handled only by the nominated IMT member, with limited access provided to other staff.
4. 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.
5. 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

The communication shall be transparent but delivered with care. Care must be taken not to disclose information that is uncertain and may change as investigation proceeds.

Information dissemination shall be central and from a dedicated war room.

Depending on the magnitude of a cyber incident, it may be necessary to brief employees of the bank 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:

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

All internal communications must be reviewed and approved by the Chief Marketing Officer, the Chief Information & Cyber Security Groupr and the Chief Digital Officer 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 CBN, NITDA, ngCERT, media houses

and the public). This is particularly important if the incident affects IT networks, systems or applications relied upon by external interested parties, such as public facing websites or services.

Key messages to consider when communicating with external stakeholders include:

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

All external communications must be reviewed and approved by the Chief Marketing Officer, the Chief Information & Cyber Security Groupr and the Chief Digital Officer. If the SEMT is activated, the SEMT Chair (or delegate) should approve all external communications prior to release.

Step 4: Recover

The Incident Management Team (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 key stakeholders from Technology group. 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 Chief Information & Cyber Security Groupr 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 Chief Information & Cyber Security Groupr.

The Chief Information & Cyber Security Groupr should gather copies of all notes taken during the response effort to assist with a Post Incident Review.

Step 5: Learn and Improve

Learn and improve is a critical and important phase in the incident response process. 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:

1. Exactly what happened, and at what times?
2. How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
3. What information was needed sooner?
4. Were any steps or actions taken that might have inhibited the recovery?
5. What would the staff and management do differently the next time a similar incident occurs?
6. How could information sharing with external parties have been improved?
7. What corrective actions can prevent similar incidents in the future?
8. What precursors or indicators should be watched for in the future to detect similar incidents?
9. 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 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 ANALYSIS – 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	

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	