FINANCIAL SERVICES COMMISSION

INSTRUCTIONS FOR THE COMPLETION OF THE CYBER INCIDENT REPORTING FORMS

Table of Contents

1. INTRODUCTION

These instructions accompany the Technology and Cyber Risk Management (TCRM) Guideline issued by the Financial Services Commission (FSC).

In view of the increasing number of cyber-attacks in the region and abroad, the importance of reporting cyber-attacks to regulators cannot be overstated. One of the roles of regulators is to promote the stability of the financial system and ensure its resilience to all types of attacks inclusive of cyber-attacks. The sharing of pertinent information about a cyber-attack with the regulator assists the regulator in foreseeing and addressing additional issues and concerns that may have major impact to the financial system locally, regionally and possibly internationally. Regulators have a responsibility to carefully consider the information submitted and respond in a manner that assists regulated financial institutions to recover from such an incident or prevent other institutions from being impacted by the same or similar cyber incident.

With the development of the Cyber Incident Reporting Template (CIRT), FIs can report and document incidents in a uniform manner that facilitates the review and study of the root causes and potential problems that can result in a cyber incident. The output from the review can provide a learning platform for all stakeholders to improve Cyber Resilience within the financial system by taking steps to further enhance the implementation of Cyber Risk management frameworks.

Further to the above, the purpose of these instructions is to guide the Financial Institution (FI) on how and when to complete the reporting template. FIs are expected to answer all questions as fulsome as possible given the information acquired about the incident.

2. SCOPE OF APPLICATION

These instructions must be applied to the reporting of a cyber security incident in accordance with the definition in the TCRM Guideline.

These instructions are also applicable where the cyber incident originates from an unregistered entity (e.g. when a cyber incident originates in the parent company or in an unregistered subsidiary) and affects the services provided by the registered entity either directly or indirectly (e.g. the capacity of the FI to execute delivery of its products and services activity is jeopardized as a result of the incident).

These instructions also apply to cyber incidents affecting functions outsourced by FIs to third parties.

3. INCIDENT CLASSIFICATION

A cyber incident can be classified as low, medium, high or critical. View the Incident Classification Matrix in the Appendix A for further details regarding the classification of incidents.

4. REPORT TEMPLATE DESCRIPTIONS

4.1 The Initial Report Template

This is the first notification that the FI submits to the FSC after it has been established and confirmed that a cyber incident has occurred.

4.2 The Intermediate Report Template

This report contains a more detailed description of the incident and its consequences. It is an update to the initial report and/or an update to a previous intermediate report on the same incident.

4.3 The Final Report Template

This is the last report the FI will submit on the incident if:

i. a root cause analysis has already been carried out and estimates can be replaced with real figures or

ii. the incident is no longer disruptive to the FI's normal operations and is contained

5. INSTRUCTIONS FOR SUBMITTING THE REPORTING TEMPLATES

5.1 The Notification Process

- When a cyber incident occurs, the FI is required to classify the incident in a timely manner but no later than within **24 hours** of its detection. A cyber incident is classified as major if it satisfies the criteria for **high** or **critical** as defined in the Classification Matrix. If the incident cannot be classified within 24 hours, the FI should inform the Relationship Officer and/or Relationship Manager immediately and communicate the reason for this in the **Initial Report.**

- Notwithstanding the above, the FSC should also be contacted promptly pending the submission of the report, as applicable:

  o Where a matter is classified as major within twenty-four (24) hours; or

- Where a matter reaches the media or social platforms.

- The report date and time refer to the exact date and time the report was submitted to the regulator.

- FIs should be prepared to submit any additional documents required by the FSC, to complement the information submitted in the template, as well as follow up on any requests or clarifications made by the regulator.

- All additional information contained in the documentation provided by the FI to the FSC should be documented in the template.

- FIs should at all times preserve the confidentiality and integrity of the information exchanged between them and the FSC.

The incident reporting forms are automatically submitted to the FSC, once the registrant clicks the "submit" button on the form. However, in extenuating circumstances or to seek guidance on any cyber-related matter, registrants should contact the FSC's cyber team via email at cyberteam@fsc.gov.bb .

5.2 The Initial Report (Form 1)

- Once a cyber incident occurs, the FI is required to complete the **Initial Report Form (Form 1**) with the information available, and submit it to the relevant sub-division.

- The initial report should be submitted within **four (4) hours** from the moment the cyber incident has been **classified as high or critical and within twenty-four (24) hours** for incidents classified as low or medium. If the email service is down, the FI should communicate this by telephone (or any other reliable back-up communication method) to the Relationship Officer and/or Relationship Manager and email the report once the email service is operational again.

- Once received by the FSC, an Incident Reference Code (IRC) will be assigned to the incident and will be communicated to the FI. The purpose of the IRC is to uniquely identify the incident. The FI would be required to populate the slot provided for this code at the top of each form.

- The initial report requires FIs to provide basic characteristics about the cyber incident and foreseen consequences based on the information available at the time. FIs are also expected to resort to estimations in instances where actual data is not available.

5.3 The Intermediate Report (Form 2)

- If the cyber incident has not been resolved **5 days** after the submission of the Initial Report, the FI is required to populate the **Intermediate Report Form (Form 2)** with the information available. Any updates to the **Initial Report Form** should also be included in the second submission.

- In the case where the cyber incident has not been resolved in **five (5)** working days after the first Intermediate report, the FI is required to submit an additional Intermediate report.

- However, notwithstanding the above, at any point after the Initial Report and the first submission of the Intermediate Report, and the issue remains unresolved, the FI will be expected to submit an additional Intermediate Report upon the request of the regulator. This request may occur before the previously identified **five (5)** day period has passed and could be a daily request as long as the cyber incident remains unresolved.

- The FI's submission of the additional Intermediate Report should always be accompanied by an updated Initial Report.

- FIs should also submit Intermediate Reports when regular business activities have been recovered and business is back to normal. FIs should consider business has resumed to normal when operations are restored with the same level of service/conditions as defined by the FI or defined externally by a service level agreement (e.g. processing times, capacity, security requirements). The resumption of business as normal also means that contingency measures are no longer in place. The Intermediate Report should contain a more comprehensive description of the cyber incident and its consequences and be accompanied by an updated Initial Report.

- As in the case with the Initial Reports, when actual data is not available, FIs are required to make use of estimations.

5.4 <u>The Final Report (Form 3)</u>

- FIs should deliver the final report, based on an independent assessment to the FSC within **twenty (20) working days** after business is deemed back to normal. FIs in need of an extension of this deadline (e.g. when there are no actual figures on the impact available or the root causes have not been identified yet) should contact the FSC's cyber team or their relationship officer before the time has elapsed and provide an adequate justification for the delay, as well as a new estimated date for the final report.

- FIs should include in their final report, full information on the following:

    - actual figures on the impact instead of estimates (as well as any other updates needed in form 1 and 2); and

    - if already known, the root cause and a summary of measures adopted or planned to be adopted to resolve the problem and prevent its reoccurrence in the future.

- FIs should ensure that the final report is accompanied by the most up-to-date versions of the Initial and Intermediate Reports.

6. DELEGATED REPORTING

- FIs wishing to delegate reporting obligations of cyber incidents to a third party, must formally write the FSC to obtain approval.

- In order to be eligible for approval, the following conditions must be met:

    - Irrespective of the possible delegation of reporting obligations, the affected FI remains fully responsible and accountable for the content of the information provided to the regulator.

    - FIs will monitor to ensure that the service is being delivered in the manner expected and in accordance with the terms of the contract or outsourcing agreement.

    - The FI should ensure and confirm the confidentiality and quality of sensitive data, as well as the consistency, integrity and reliability of the information to be provided to the FSC.

- FIs are required to inform the FSC of any material developments affecting the designated third party and its ability to fulfil the reporting obligations.

- FIs are required to diligently fulfil their reporting obligations without any recourse to external assistance whenever the designated third party fails to inform the FSC of a cyber security incident.

7. UPDATE TO CYBER SECURITY POLICIES AND PROCEDURES

FIs should ensure that their cyber security policies clearly define all the responsibilities for cyber incident reporting as well as the processes implemented in order to fulfil the requirements defined in these Instructions.

8. INSTRUCTIONS TO POPULATE THE FORMS

FORM 1 – INITIAL REPORT

Access Form 1

Form 1 – Initial Report	
General Details	
Type of Report	• Solo: the report refers to a single FI • Consolidated: the report refers to a FI and its branches and subsidiaries that are also licensed institutions and are governed under the same Enterprise Cyber Security Framework • List of Entities in Consolidated Report: Applicable only if Consolidated reporting is selected and refers to the FIs affected by the incident that are branches or subsidiaries of the parent entity affected.
Name of Entity	• FI that is experiencing the cyber incident
Name of parent entity, if applicable	• In the case of groups of entities, please indicate the name of the parent entity.
Country/countries affected by the incident	• Country or countries where the impact of the incident has materialized *(e.g. several branches of the FI located in different countries are affected)*, irrespective of the severity of the incident in the other country/countries. • If the country is not listed, select **other** and type the name of the country in the space provided
Primary Contact Person	• Name and surname of the person responsible for reporting the incident. • Email: email address to which any requests for further clarifications could be addressed, if needed. It ought to be a corporate email address. • Telephone: telephone number through which any requests for further clarifications could be addressed, if needed. It ought to be a corporate telephone or cell number.

Secondary Contact Person	• Name and surname of an alternative person that could be contacted by the FSC to inquiry about an incident when the primary contact person is not available. In the case of a third-party service provider reporting on behalf of the affected FI, name and surname of an alternative person in the incident management/risk department or similar area. • Email: email address to which any requests for further clarifications could be addressed, if needed. It ought to be a corporate email address. • Telephone: telephone number through which any requests for further clarifications could be addressed, if needed. It ought to be a corporate telephone or cell number.
Reporting Entity *(if reporting entity is a third party)* **Primary Contact Person** **Secondary Contact Person** **Email** **Telephone**	• (primary) In the case of a third-party service provider reporting on behalf of the affected FI, the name and surname of the **person** responsible for reporting the incident. • (secondary) In the case of a third-party service provider reporting on behalf of the affected FI, the name and surname of the **alternative person** responsible for reporting the incident. (primary & secondary) • Email: email address to which any requests for further clarifications could be addressed, if needed. It ought to be a corporate email address. • Telephone: telephone number through which any requests for further clarifications could be addressed, if needed. It ought to be a corporate telephone or cell number.
Form 1: Incident Detection and Classification	
Date and time of detection of the incident	Date and time when the incident was first identified.
Initial Classification of Incident	Select classification based on the criteria defined in the Classification Matrix.
Date and time of classification of the incident	Date and time when the cyber security incident was classified.

The Incident was detected by	Indicate whether the incident was detected by an internal user, (e.g. a general staff member, internal audit) or by another external party (e.g. customer, perpetrator). If it was none of those, please select other and provide an explanation in the corresponding field.
Type of incident	Choose from the list provided, the best indication with the information available, the type of incident that has occurred. If no selection can be made, select **other** and type the incident and a brief description.
Criteria Triggering the Report	Indicate which of the criteria have triggered the incident report. Tick all that apply. Select **other** and state trigger if not observed in the list provided.
Short Description of the Incident	Explain briefly the most relevant issues of the incident, covering possible causes, immediate impacts, details of any unusual customer activity, etc.
Please state whether the incident was or will be reported to other regulatory authorities	Indicate whether the cyber incident has been/will be reported to other authorities under separate incident reporting frameworks, if known at the time of reporting. If so, kindly specify the respective authorities.
Reasons for the late submission of the Initial Report (where applicable)	Explain the reasons why you required longer than 24 hours to classify the incident.

FORM 2 – INTERMEDIATE REPORT

Access Form 2

Form 2 – Intermediate Report - General Details	
Who was the threat actor?	Identify the category of the person or group that orchestrated the incident. Please refer to the table ***"Threat Actor Types"*** for further guidance.
What was the motive?	Indicate the reason behind the cyber-attack.
What was the level of internal escalation of the incident?	Detail your incident escalation process including, for example, levels of escalation, persons responsible for escalation, the person to whom the incident is being escalated and any associated time frames.
How did the incident start?	Detail what actions led to the incident and provide a brief overview of the initial impact. Also include relevant details e.g. any unusual customer activity.
How did the incident evolve?	Detail how did the incident spread throughout your network
Was the incident communicated to public, customers and staff? If yes, please specify	Specify the persons to whom the incident was communicated and the communication message.
Was crisis management started (internal and/or external)?	Detail what steps were taken during the crisis and the responders involved both internally and externally.
Form 2 – Intermediate Report – Incident Classification	
Type of incident	Refer to the table ***"Type of Incidents"*** for examples.
Cause of Incident	Select from the list of probable causes. Multiple choices may be selected.
Form 2 – Intermediate Report – Incident Scope	
Type of data disruption	Indicate how the data was disrupted. Select all that apply. • Integrity: the accuracy and completeness of the asset or data. • Availability: the accessibility of data according to acceptable predefined levels. • Confidentiality: information is not made available to unauthorized persons, entities, or processes.
Functional areas affected	Specify how each applicable functional area was affected. Mentioning any data access challenges, systems malfunction etc.
Service Channels affected	Indicate the channel or channels of interaction with customers that have been affected by the cyber incident. Multiple selections can be made.
Form 2 – Intermediate Report – Incident Severity	
Transactions affected	Impact level: refer to the Classification matrix
Form 2 – Intermediate Report – Incident Mitigation	
Which actions/measures have been taken so far or are planned to recover from the incident?	Detail any forensic activity, strategies and resources, both technical and human, used in recovery

FORM 3 – FINAL REPORT

Access Form 3

Form 3 – Final Report – General Details	
Updates made to previous initial and intermediate reports	Provide further details on the cyber incident including in particular, any changes made to the information previously provided in the intermediate report.
Are all original controls in place?	Indicate whether or not the FI had to cancel or weaken some controls at any time during the cyber incident. If so, indicate whether these controls are back in place and if not, explain why and outline the steps and timeframe required for restoration.
Form 3 – Final Report – Root Cause Analysis and follow up	
What was the root cause?	Indicate what the root cause of the incident was, or if not known, what it was most likely to have been. Multiple choices may be selected. Description of the selections can be observed under ***"Appendix 1: Types of Root causes".*** Also note that the root cause must be distinguished from the impact.
If Other root cause	If the cause of the cyber incident is none of the above, further details should be provided in the free text field.
Other relevant information on the route cause	Provide any other details on the root cause including preliminary conclusions drawn from the analysis
Main corrective actions or measures taken or planned to be taken to prevent the event from reoccurring	Describe the actions that have been taken or planned to be taken in order to prevent a possible reoccurrence of the cyber incident.
Form 3 – Final Report – Additional Information	
Has the incident been shared with other financial institutions for information purposes?	Provide an overview of which FIs have been reached out to and details of the information given to them. Ensure to note what was shared and why.
Has any legal action been taken against the financial institution?	Indicate whether at the time of filing of the report if there has been any legal action due to the occurrence of the cyber incident.
Assessment of the effectiveness of the action taken?	Include a self-assessment of the effectiveness of the actions taken during the duration of the cyber incident, including any lessons learnt.

9. APPENDIX A – INCIDENT CLASSIFICATION MATRIX

		SEVERITY			
		Low	**Medium**	**High**	**Critical**
		• No impact or minimal impact to the delivery of services and products to customer bases • Downtime spans minutes • Recovery time is predicted and can be handled internally • No incident contagion • No notification from service providers • Data users may encounter none to little inconveniences relating to data integrity and availability • Little to no impact on reputation; none to minimal cost and effort to recover • Little to no financial loss	• Minimal impact to delivery of services and products to customer base • Downtime spans 4 hours or less • Recovery time is predicted and can be remedied internally with minimal external support • Incident is contained within a unit/department • Service Provider reports minor incident detected but contained and remedied in under 4 hours • Data users may encounter significant inconveniences relating to data integrity and availability which may be corrected at low costs for licensee • Reputation moderately affected requiring moderate cost and effort to recover; moderate impact on revenue, customer base and/or staff • Financial losses can be absorbed	• Material impact to the delivery of services and products to customer base • Downtime spans above 4 hours • Recovery time is unpredictable and requires internal and extensive external support • Incident spans the entire licensee network • Service Provider reports material incident detected that has compromised its ability to offer reliable or substantial service to licensee • Data users may encounter significant consequences relating to data confidentiality, integrity or availability which may be corrected at great costs for licensee • Reputation severely damaged requiring great costs and effort to recover; severe impact on revenue, customer base and/or staff • Financial losses compromise liquidity or normal conduct of operations	• Unable to deliver services and products to customer base • Downtime spans multiple days • Critical Systems extensively compromised and threatens recoverability • Incident also compromises third party service providers and other financial institutions • Service Provider is non-operational • Data users may encounter irreversible consequences relating to data confidentiality, integrity or availability, equating to insurmountable financial losses • Reputation irrevocably destroyed; critical impact on revenue, customer base and/or staff • Financial distress or insolvency
FREQUENCY	**Low** Occurs on a yearly basis				
	Medium Occurs quarterly to bi-annually				
	High Occurs daily to monthly				

10. APPENDIX B – SPECIMEN FORMS

SPECIMEN 1

FINANCIAL SERVICES COMMISSION

Form 1 - Cyber Incident Initial Report

Within 4 hours after classification of the incident as high or critical. Within 24 hours after classification of the incident as medium or low.

Report Date:	Report Time:	Incident Report Reference Number:
9/19/2024	10:00 AM	

1. INITIAL REPORT - GENERAL DETAILS

The below table provides guidance to complete this section of the form:

SPECIMEN 1

Source of Detection of Incident

User	Details	Description
Internal User	IT/Information security function	discovered by a dedicated security team or specialized consultants.
	Internal Audit	discovered following a review by internal auditors.
	General Staff	reported by temporary or permanent staff.
	System detection	discovered using automated tools.
External User	Actor Disclosure	informed by perpetrator.
	Authority/Agency/Association	reported by competent authority or body.
	Law Enforcement	reported by domestic, regional, or international law enforcement.
	Customer	reported by customer of your institution.
	Peer	reported by another institution in the sector.
	Audit	discovered following a review by external auditors.
	System detection	informed by an external monitoring service tool.
	Unknown	reported by an anonymous or unidentified external entity.
	Third Party	reported by service provider, vendor, or other external dependencies.
	Unrelated party	reported by a party with no relationship to your institution.

Type of Report:

Solo

List of Entities in Consolidated Report

N/A

Insert List

Name of entity:

ABC Insurance Company Ltd.

Insert Name

Name of parent entity, if applicable:

N/A

Insert Name

Country/Countries affected by the incident:

- ☑ Barbados
- ☐ Antigua & Barbuda
- ☐ St. Maarteen
- ☐ St. Vincent & the Grenadines
- ☐ St. Kitts & Nevis
- ☐ Guyana
- ☐ Grenada
- ☐ Dominica
- ☐ Anguilla
- ☐ Jamaica

SPECIMEN 1

☐ St. Lucia ☐

☐ Trinidad & Tobago

☐

Primary Contact Person:

Jane	Doe
First	Last

Email jdoe@abcinsltd.com

Telephone: 987-3458

Phone

Secondary Contact Person

John	Browne
First	Last

Email jbrowne@abcinsltd.com

Telephone: 983-2489

Phone

Reporting entity (if reporting entity is a third party)

Primary Contact Person:

N/A	N/A
First	Last

Email:

Telephone:

Phone

Secondary Contact Person:

First Last

Email:

Telephone:

Phone

2. INCIDENT DETECTION AND CLASSIFICATION

Date of detection of incident 9/19/2024

Time of detection of incident 8:00 AM

Initial Classification of incident Critical

Date of Classification of the

Time of Classification of the

SPECIMEN 1

incident	Incident
9/19/2024	9:00 AM

The incident was detected by:	Type of Incident:
Internal User	Data Breach

Criteria triggering the report (Tick all that apply)

☐ Transactions Affected	☑ Service Downtime
☐ Financial Impact	☑ Reputational Impact
☑ Internal Users Affected	☑ Breach of Security or Information Systems
☑ High Level Internal Escalation	☑ External parties potentially affected

☑ A ransom payment was demanded.

A short description of the incident (include suspected cause and initial impact)

A phishing attempt was activated via an employee within the company. Our systems are now compromised and we are unable to access critical business functions. The attacker is also requesting a payment in order for us to regain access to our system.

Insert here

Please state whether the incident was or will be reported to other regulatory or enforcement authorities (if applicable)

Yes, Data Protection Commissioner

Insert here

Reasons for the late submission of the initial Report (if applicable)

N/A

Insert here

SPECIMEN 2

FINANCIAL SERVICES COMMISSION

Form 2 - Cyber Incident Intermediate Report

Maximum of 5 working days from the submission of the initial report.

Report Date:	Report Time:	Incident Report Reference Number:
26/09/2024	10:00 am	CI-INS-00

1. INTERMEDIATE REPORT - GENERAL DETAILS

The below table provides guidance to complete this section of the form.

SPECIMEN 2

Threat Actor Types

Category	Examples
Internal	Executive Customer-facing employee Technology staff Other staff
External	Unaffiliated person Customer Competitor Organized or professional criminal group Relative or acquaintance of employee Nation state Activist group Other
Third Party	ICT provider Other service provider Intragroup entity Other

a. Who was the threat actor?

External

b. What was the motive?

Financial

c. How did the incident start?

A phishing link was sent to an employee at our company. The employee mistakenly clicked the link which activated the attack.

Insert here

d. How did it evolve?

After the link was activated, we experienced a total shutdown of our systems where all of our core systems were compromised. 30 minutes after, there was a call made to our telephone system requesting a payment of US$90 million in order to regain access to our system.

SPECIMEN 2

Insert here

e. What was the level of internal escalation of the incident?

The incident was escalated to our senior management team.

Insert here

f. Was the incident communicated to public, customers and staff?

Yes

select

g. If yes, please specify:

Given that our entire system was shutdown, we held an in-person meeting with our staff to inform them of the situation. After the submission of our initial report to the Commission, we also held a news briefing to alert the public and by extension our customers.

Insert here

h. Was the incident communicated to enforcement authorities?

No

select

i. If yes, please specify:

N/A

Insert here

j. Was it related to a previous incident/s?

No

select

k. If yes, please specify:

N/A

Insert here

l. Were service providers/third parties affected or involved?

No

select

m. If yes, please identify them:

N/A

Insert here

n. Was crisis management started (internal and/or external)?

Yes

select

o. If yes, please specify:

We started to implement our crisis management plan

SPECIMEN 2

Insert here

p. Date and time affected systems, services and/or users were under control:

25/09/24 10:00 PM

DD/MM/YYYY HH:MM

q. Changes made to previous reports:

N/A

Insert here

2. INCIDENT CLASSIFICATION

The below table provides guidance to complete this section of the form.

Type of Incidents

Incident Type	Definition	Examples
Business Disruption	Any type of internal or external incident that disrupts the provision of an entity's services	Technology failure, loss of third-party service, Denial of Service (DOS), malware
Compromise	Violation of the security of an information system	Account compromise, email compromise, intrusion, defacement
Data Breach	Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to data transmitted, stored, or otherwise processed	Data leakage, data loss
Financial Theft/Fraud	A deliberate act to obtain unauthorised financial benefit	Theft of funds via digital channel
Information Disorder	The spread of false or reality-based information, whether malicious or not	Misinformation, disinformation, malinformation

a. Type of Incident:

Compromise

select

b. Cause of Incident:

☐ Under investigation

☐ System failure

☐ Malicious action

☑ Human errors

SPECIMEN 2

☐ Process failure ☐ External events

☐

c. If other, please specify:

Insert here

3. INCIDENT SCOPE

a. Type of data disruption:

☑ Integrity ☑ Availability ☑ Confidentiality

b. Functional areas affected:

☐ Deposit-taking ☐ Capital markets and investment activities

☐ Lending ☑ Payments, clearing, custody and settlement

☐

c. Please specifiy the affected functional areas:

Customers are unable to pay their premiums, receive quotations and generally make contact with us.

Insert here

d. Service channels affected:

☑ Branches ☐ Telephone Banking

☐ E-banking ☐ Mobile Banking

☐ ATMs

☑ Online portal, email and telephone access

e. If other, please specify:

N/A

Insert here

f. Provide any other relevant details:

SPECIMEN 2

Insert here

3. INCIDENT SEVERITY

Transactions affected

a. Impact level:

N/A

b. Number of transactions affected

Insert here

c. As a % of number of total transactions

Insert here

d. Value of transactions affected in BBD

Insert here

Breach of security of network or information systems

e. Impact level:

High

f. Describe how the network or information systems have been affected:

Our access to our network and information systems was also restricted.

Insert here

Service downtime

g. Impact level:

High

h. Total Service downtime (Insert days, hours and minutes):

4 days

Insert here

Financial Impact

i. Impact level:

N/A

j. Direct costs in BBD

Insert here

k. Indirect costs in BBD

Insert here

Third party providers or other financial institutions affected

l. Impact level

SPECIMEN 2

N/A

m. Describe the impact:

Insert here

Reputational Impact

n. Impact level

High

o. Describe the impact:

Customers were unable to be appropriately serviced for 4 days. As a result, this negatively impacted our reputation.

Insert here

4. INCIDENT MITIGATION

p. Which actions/measures have been taken so far or are planned to recover from the incident?

Our IT Team was able to recover our systems without the payment of the ransom. We will ensure staff undergo mandatory Cybersecurity awareness training every 6 months.

Insert here

q. Has the Business Continuity Plan and/or Disaster Recovery Plan been activated?

Yes

select

r. If so, when? (DD/MM/YYYY, HH:MM)

20/09/24, 7:00 AM

DD/MM/YYYY, HH:MM

s. If so, please describe:

The day after we reported the incident, our disaster recovery plan was activated to ensure the incident was contained in a timely manner.

Insert here

SPECIMEN 3

FINANCIAL SERVICES COMMISSION

Form 3 - Cyber Incident Final Report

Within 20 working days after the submission of the intermediate report

Report Date:	Report Time:	Incident Report Reference Number:
24/10/2024	10:00 am	CI-INS-00

1. General Details

Update of the information from the initial report and the intermediate report(s).

a. Updates made to previous initial and intermediate reports

N/A

Insert here

b. Any other relevant information (if applicable)

N/A

Insert here

c. Are all original controls in place?

SPECIMEN 3

Yes

d. If no, specify which controls and the additional period required for their restoration

N/A

Insert here

2. Root Cause Analysis and Follow up

The below table provides guidance to complete this section of the form.

Appendix 1: Types of Root causes

Malicious Action

External or internal actions intentionally targeting the licensee. The categories are as follows:

Malicious Code	a virus, worm, trojan, spyware
Information gathering	scanning, sniffing, social engineering
Intrusions	privileged account compromise, unprivileged account compromise, application compromise, bot
Distributed/Denial of service attack (D/Dos)	An attempt to make an outline service unavailable by overwhelming it with traffic from multiple sources.
Deliberate internal actions	E.g. sabotage, theft
Deliberate external physical damage	E.g. sabotage, physical attack of the premises/data centres
Information content security	Unauthorised access to information, unauthorised modification of information
Fraudulent actions	Unauthorised use of resources, copyright, masquerades, phishing

SPECIMEN 3

Process Failure

The cause of the incident was a poor design or execution of the payment process, the process controls and /or the supporting processes, e.g. process for change/ migration, testing, configuration, capacity, and monitoring. The categories are as follows:

Deficient monitoring and control	E.g. in relation to running operations, certificate expiry dates, licence expiry dates, patch expiry dates, defined maximum counter values, database fill levels, user rights management, dual control principle.
Communication issues	E.g. between market participants or within the organisation
Improper operations	E.g. no exchange of certificates, cache is full.
Inadequate Change management	E.g. unidentified configuration errors, roll-out including updates, maintenance issues, unexpected errors.
Inadequacy of internal procedures and documentation	E.g. Lack of transparency regarding functionalities, processes and occurrence of malfunctioning, absence of documentation
Recovery issues	E.g. contingency management, inadequate redundancy

SPECIMEN 3

System Failure

The cause of the incident is associated with an inadequate design, execution, components, specifications, integration or complexity of the systems, networks, infrastructures, and databases that support the payment activity. The categories are as follows:

Hardware failure	Failure of physical technology equipment that runs the processes and/or stores the data needed by licensees to carry out their payment-related activity (e.g. failure of hard drives, data centres, and other infrastructure
Network failure	Failure of telecommunications networks, either public or private, that allow the exchange of data and information (e.g. via the internet) during the service activity.
Database issues	Data structure which stores personal and payment-related information needed to execute payment transactions.
Software/application failure	Failure of programs, operating systems, etc. that support the provision of banking or business services by the licensee.
Physical damage	For example, unintentional damage caused by inadequate conditions or construction work.

Human Error

The incident was caused by the unintentional mistake of a person, be it as part of the business procedure (e.g. uploading wrong data) or related to it somehow (e.g the power is accidentally cut off and the business activity is put on hold). The categories are as follows:

Unintended	E.g. mistakes, errors, omissions, lack of experience and knowledge
Inaction	E.g. due to lack of skills, knowledge experience, awareness
Insufficient resources	E.g. lack of human resources, availability of staff

SPECIMEN 3

External Event

The cause is associated with events generally outside the organisation's control. The categories are as follows:

Failure of a supplier/technical service provider	E.g. power outage, Internet outage, legal issues, business issues, service dependencies
Force majeure	E.g. power failure, fires, natural causes such as earthquakes, floods, heavy precipitation, heavy wind

e. What was the root cause? (multiple choices may be selected)

☑ Malicious Action
☑ Human Failure
☐ Process Failure
☐ External Event
☐ System Failure

f. Please specify the options identified aboved:

The incident occurred because a malicious link was sent to one of our employees. Once the employee clicked the link, the attack commenceD.

Insert here

g. If other root cause, please specify:

N/A

Insert here

h. Other relevant information to the root cause:

N/A

Insert here

i. Main corrective actions/measures taken or planned to prevent the incident from reoccuring:

We have blocked suspicious emails from our employees general inbox and redirected them to spam, increased staff awareness and training.

Insert here

3. Additional Information

j. Has the incident been shared with other Financial Institutions for information purposes?

No

SPECIMEN 3

k. If Yes, please provide details:

Insert here

l. Has any legal action been taken against the Financial Instutution?

No

m. If yes, please provide details:

Insert here

n. Was a self-assessment of the effectiveness of the remedial actions conducted?

Yes

o. If Yes, please provide details highlighting lessons learnt:

We reviewed our remediation measures and determined that greater communication is needed if a similar incident should occur. We have now developed an internal and external communications team to handle this process. We have also included provisions for regular simulation exercises to test our security mechanisms to ensure robustness.

Insert here