INSURANCE COMMISSION
OF THE BAHAMAS

CYBERSECURITY INCIDENT REPORTING FORM FOR LICENSEES

Purpose

The Insurance Commission of The Bahamas is introducing a Cybersecurity Incident Reporting Form to facilitate its awareness of and response to cybersecurity incidents involving all regulated Licensees.

Initial Notification Requirements

1. All companies are responsible for addressing cybersecurity incidents in a timely and effective manner. They are required to notify the Commission within *24 hours* of becoming aware of a cyber-incident.
2. Companies should complete the Cybersecurity Incident Report template below and submit it to the Commission within 72 hours of the incident. Where specific details are unavailable at the time of the initial report, the Company must indicate 'information not yet available.' In such circumstances, the Company must provide the best estimates and all other details available, including their expectations of when additional information will be available.

Subsequent Reporting Requirements

1. The Commission expects the Company to provide regular updates as new information becomes available until the Company provides all details about the incident.
2. Following incident containment, recovery, and closure, the Company should report to the Commission on its post-incident review and lessons learned.

Failure to Report

Failure to report incidents as outlined above may result in increased supervisory oversight, including, but not limited to, enhanced reporting by the Company and/or issuance of compliance directions as relevant.

Please complete this form to provide an accurate account of the incident as of the current date. Ensure to include all required information to assist with a comprehensive review. If additional space is needed, attach supplementary documents clearly labeled with the relevant details.

All submissions must be accurate and thorough to facilitate proper evaluation and response.

NOTE: Intentional misstatement or failure to disclose information may constitute an offence.

Section A – Details of the Licensee or Registrants
Licensee Name:
License ICB Number:
Address:
Reporting Person:
Reporting Person Email:
Reporting Person Phone Number:
Date of Report Submission:
Type of Report: ☐ Initial Report ☐ Follow-up Report ☐ Final Report

Section B – System Details
Information/security services outsourced: ☐ Yes ☐ No
If yes, please name company:
Were any containment measures made? ☐ Yes ☐ No
If yes, describe:

INCIDENT DETAILS

Section C – Incident Overview
Date and Time of Discovery: [MM/DD/YYYY, HH]:

Date and Time of Occurrence (if known): [MM/DD/YYYY, HH]:
Type of Incident: ☐ Data Breach ☐ Ransomware ☐ Phishing Attack ☐ Denial of Service (DoS) ☐ Insider Threat ☐ Malware Infection ☐ Other (Specify): ***[Describe]***

Section D – Description of the Incident
Provide a brief description of the incident, how it was discovered, and any relevant background information. ***[Provide details about how the breach occurred, initial discovery, and key events in the incident.]***
Section E – Nature of Compromised Data (if applicable)

Type of Data Affected:

- ☐ Personal Identifiable Information (PII)
- ☐ Financial Information
- ☐ Health Records
- ☐ Intellectual Property
- ☐ Business Confidential Information
- ☐ Other (Specify): ***[Describe]***

Estimated Number of Individuals/Records Affected [Number, if known]:

Section F – Systems Affected

Provide a brief description of the systems affected, including software or hardware impacted.

Description: [Provide names of systems, databases, or services compromised and the extent of impact.]

RESPONSE AND MITIGATION ACTIONS

Section G – Immediate Actions Taken

Summarize immediate actions taken upon discovery of the incident (e.g., implementation date, containment, isolation of systems, password resets).

Description: [Describe actions taken to mitigate the incident.]

Section H – Planned Future Taken

Describe planned actions for ongoing mitigation, investigation, and prevention.

Description: [Describe additional steps planned to address the incident and prevent recurrence, inclusive of implementation dates and timelines.]

Section I – Notifications to Other Entities
Was Law Enforcement notified: ☐ Yes ☐ No Specify Agency:
Were the affected customers or individuals notified: ☐ Yes ☐ No Specify how notification was provided:
Were other regulatory bodies notified: ☐ Yes ☐ No Specify which bodies were notified:
Have you retained legal counsel: ☐ Yes ☐ No Specify the firm:
Have you retained an independent cybersecurity solution: ☐ Yes ☐ No Specify the firm:

Section J – Expected Business Impact
Provide an assessment of the potential impact on business operations and clients. ***Description: [Describe how the breach may impact your company's ability to provide services.]***

SUPPORTING DOCUMENTATION

Section K – Attachments (If applicable)
Please attach any relevant documents (e.g., incident logs, forensic reports, vulnerability assessments). **List of Attachments:** • Attachment name 1: • Attachment name 2: • Attachment name 3: • Attachment name 4:

Declaration:

"I hereby confirm that the information provided in this report is accurate and complete to the best of my knowledge."

Signature: _____

Printed Name: _____

Title: _____

Date: _____

(Revised September 2025)