CENTRAL BANK OF SRI LANKA
BANK SUPERVISION DEPARTMENT

07 May 2025 **CIRCULAR** **No. 02 of 2025**

REPORTING OF INFORMATION TECHNOLOGY AND CYBERSECURITY INCIDENTS OF LICENSED BANKS

The Central Bank of Sri Lanka (CBSL) having observed the increased reliance on digital infrastructure by licensed banks, the risk of cyberthreats, data breaches, and system failures that require prompt and transparent reporting of such incidents to CBSL and relevant stakeholders to ascertain risks, mitigate potential disruptions and safeguard customer information and assets, hereby issues this Circular to licensed commercial banks and licensed specialised banks (herein after referred to as "licensed banks") with a view to ensuring the operational resilience of licensed banks in Sri Lanka. This Circular is issued further to the requirements stipulated in the Banking Act Direction No. 16 of 2021 on "Regulatory Framework on Technology Risk Management and Resilience for Licensed Banks, as amended".

2. **Definitions**: For the purpose of this Circular, the following definitions are applicable:
   - 2.1 **Information Technology (IT) incident:** An event which causes operational disruption, potential financial losses, and reputational damage to a licensed bank due to failures or security breaches in the IT systems of such licensed bank.
   - 2.2 **Cybersecurity incident:** An event that compromises the confidentiality, integrity or the availability of systems and information of a licensed bank.
   - 2.3 **Online and digital scams:** A fraudulent activity performed using the internet and digital devices to deceive individuals into revealing personal, financial, or other sensitive information or losing their money.

3. **Categorisation of IT and cybersecurity incidents:** At a minimum, following broad categories of IT and cybersecurity incidents and any other such incident shall be reported to CBSL.

   - 3.1 Intrusion/ Hacking, Malware, Ransomware, Malicious Code, Virus, Phishing, Distributed Denial of Service (DDoS) Attacks, Social Engineering, Unauthorized

System Usage, Insider Threats, Advanced Persistent Threats (APTs) and Supply Chain Attacks

3.2 Online or digital scams affecting the customers

3.3 Unplanned critical system outages/ interruptions/ failures/ slowness/ unresponsiveness

3.4 Regulatory non-compliances relating to IT and cybersecurity requirements

4. **Regulatory reporting:** Licensed banks are required to report the above incidents to the Director, Bank Supervision Department via techrisk.bsd@cbsl.lk, copying dbsd@cbsl.lk as directed in the Table 01 hereto.

Table 01: Reporting IT and Cybersecurity Incidents

Template Ref.	Type of the Report	Timelines for Reporting
Annex 01	Immediate reporting	Within 2 hours of detection of the incident
Annex 02	Detailed reporting	Within 14 days of detection of the incident
Annex 03	Quarterly reporting	Within 15 days following the end of each quarter

5. **Revocation:** Circular dated 25.01.2016 on "Reporting on Cybersecurity Events" is hereby revoked with immediate effect.

Mrs. R R S De Silva Jayatillake
Director of Bank Supervision

Annex 01

REPORTING INFORMATION TECHNOLOGY AND CYBER SECURITY INCIDENTS
(Template for Immediate Reporting)

Information on the Incident	
1. Name of the bank	
2. Details of the incident	
2.1 Date and time of detection	
2.2 Type of the incident [a]	
2.3 Physical location/ branch *(if applicable)*	
2.4 Brief summary of the incident	
2.5 Root cause *(if identified)*	
2.6 Immediate actions taken by the bank *(if any)*	
2.7 Internal reporting authority [b] *(including initial the date of notification)*	
2.8 Whether the incident has been reported to any other authority? [c] If yes, Name of the authority: Date and time of reporting:	
3. Date and time of reporting to BSD	
4. Key contact person of the bank	
4.1 Name	
4.2 Designation	
4.3 Contact number & email address	
Preliminary Impact Assessment in Summary [d]	
5. Business impact	
6. Data and information security impact	
7. Impact on stakeholders and customers	
8. Reputational impact	
9. Regulatory or legal impact	
10. Financial impact	

Guidelines for reporting:

Licensed Banks are required to submit the details as per the attached format within 2 hours of detection to the Director of Bank Supervision via techrisk.bsd@cbsl.lk, copying dbsd@cbsl.lk, based on the availability of the information considering the timeline for reporting.

[a] Categories of Incidents:

(i) Intrusion/ Hacking, Malware, Ransomware, Malicious code, Virus, Phishing, Distribute Denial of Service (DDoS) Attacks, Social Engineering, Unauthorized System Usage, Insider Threats, Advanced Persistent Threats (APTs) and Supply Chain Attacks
(ii) Unplanned critical system outages/ interruptions/ failures/ slowness/ unresponsiveness
(iii) Online or digital scams affecting the customers
(iv) Regulatory compliance failures
(v) Any other technology or cyber related event

[b] To whom the event has been internally escalated:

(i) Chief Information Security Officer
(ii) Chief Information Officer
(iii) Chief Executive Officer
(iv) Information Security Committee
(v) Board Integrated Risk Management Committee
(vi) Board of Directors

[c] Whether this incident was reported to:

(i) Sri Lanka Computer Emergency Readiness Team (SLCERT)
(ii) Financial Sector Computer Security Incident Response Team (FinCSIRT)
(iii) Payment and Settlement Department of Central Bank of Sri Lanka
(iv) Computer Crime Investigation Division (CCID)
(v) Any other relevant legal authorities

[d] Impact Assessment may include the following:

Business Impact	• Disruption to banking services • System downtimes • Operational delays
Data and Information Security Impact	• Compromise of customer data • Unauthorized access to sensitive information • Breach of confidentiality, integrity, or availability
Stakeholders' and Customer Impact	• Number of affected customers and accounts • Disruptions in communication and service delivery • Customer complaints and potential compensations
Reputational Impact	• Is this incident likely to attract media attention? • Loss of customer trust and confidence • Impact on investor and stakeholder relations
Regulatory or Legal Impact	• Potential legal liabilities and penalties
Financial Impact	• Include the estimated/ actual loss to the bank/ customers/ stakeholders, separately

Annex 02

REPORTING INFORMATION TECHNOLOGY AND CYBER SECURITY INCIDENTS
(Template for Detailed Reporting)

Information on the Incident	
1. Name of the bank	
2. Initial date and time of reporting of the incident to BSD	
3. Details of the incident	
3.1 Date, time and the duration of the incident	
3.2 Type of the Incident [a]	
3.3 Physical location/ branch *(if applicable)*	
3.4 Internal reporting authority [b] *(including initial date of notification)*	
3.5 Whether the incident has been reported to any other authority? [c] If yes, Name of the authority: Date and time of reporting:	
3.6 Whether this incident has been informed to the stakeholders/ customers of the bank. *(if yes date and time of reporting)*	
4. Key contact person of the bank	
4.1 Name	
4.2 Designation	
4.3 Contact number & email address	
Detailed Root Cause Analysis	
5. Factors that caused the problem/ reasons for occurring	
6. Immediate actions taken by the bank to address the root cause	
7. Interim actions taken by the bank to address the root cause	
Impact Assessment [d]	
8. Business impact	
9. Data and information security impact	
10. The impact on stakeholders and customers	
11. Reputational impact	
12. Regulatory or legal impact	
13. Financial impact	
Final Assessment	
14. List the corrective actions taken to prevent future occurrences of similar types of incidents	
15. Target dates for the corrective actions *(if any)*	

Guidelines for reporting:

Licensed Banks are required to submit the full details as per the attached format with any supporting documents within 14 working days of detection to the Director of Bank Supervision via techrisk.bsd@cbsl.lk, copying dbsd@cbsl.lk.

[a] Categories of Incidents:

(i) Intrusion/ Hacking, Malware, Ransomware, Malicious code, Virus, Phishing, Distribute Denial of Service (DDoS) Attacks, Social Engineering, Unauthorized System Usage, Insider Threats, Advanced Persistent Threats (APTs) and Supply Chain Attacks
(ii) Unplanned critical system outages/ interruptions/ failures/ slowness/ unresponsiveness
(iii) Online or digital scams affecting the customers
(iv) Regulatory compliance failures
(v) Any other technology or cyber related event

[b] To whom the event has been internally escalated:

(i) Chief Information Security Officer
(ii) Chief Information Officer
(iii) Chief Executive Officer
(iv) Information Security Committee
(v) Board Integrated Risk Management Committee
(vi) Board of Directors

[c] Whether this incident was reported to:

(i) Sri Lanka Computer Emergency Readiness Team (SLCERT)
(ii) Financial Sector Computer Security Incident Response Team (FinCSIRT)
(iii) Payment and Settlement Department of Central Bank of Sri Lanka
(iv) Computer Crime Investigation Division (CCID)
(v) Any other relevant legal authorities

[d] Impact Assessment shall inter alia include the following:

Business Impact	• Disruption to banking services • System downtimes • Operational delays
Data and Information Security Impact	• Compromise of customer data • Unauthorized access to sensitive information • Breach of confidentiality, integrity, or availability
Stakeholders' and Customer Impact	• Number of affected customers and accounts • Disruptions in communication and service delivery • Customer complaints and potential compensations
Reputational Impact	• Is this incident likely to attract media attention? • Loss of customer trust and confidence • Impact on investor and stakeholder relations
Regulatory or Legal Impact	• Potential legal liabilities and penalties
Financial Impact	• Include the estimated/ actual loss to the bank/ customers/ other stakeholders, separately

Annex 03

REPORTING INFORMATION TECHNOLOGY AND CYBER SECURITY INCIDENTS
(Template For Quarterly Reporting)

Name of the Bank :

Report as at Q _ 20_ _

	Incident 1	Incident 2	.....
1. Type of incident [a]			
2. Summary of the incident			
3. Date and time of the occurrence			
4. Date of detection			
5. Physical location/ branch (if applicable)			
6. Root cause of the incident			
7. Corrective actions taken by the bank			
8. Impacted party (bank, customer, any other stakeholder)			
9. Estimated/ actual impact of the incident (financial and operational) [b]			
10. Amount recovered by the bank			
11. Internal reporting authority [c]			
12. Has the incident been reported to any other authority, if so name			
13. Law enforcement authorities involved (if applicable) [d]			

Reported by:

Name:

Designation:

Date:

Guidelines:

[a] Categories of Incidents:

(i) Intrusion/ Hacking, Malware, Ransomware, Malicious code, Virus, Phishing, Distribute Denial of Service (DDoS) Attacks, Social Engineering, Unauthorized System Usage, Insider Threats, Advanced Persistent Threats (APTs) and Supply Chain Attacks
(ii) Unplanned critical system outages/ interruptions/ failures/ slowness/ unresponsiveness
(iii) Online or digital scams affecting the customers
(iv) Regulatory compliance failures
(v) Any other technology or cyber related event

[b] Please provide the amount of loss to the bank/ customers or any other stakeholder in case of financial impact and description in case of operational impact.

[c] To whom the event has been internally escalated:

(i) Chief Information Security Officer
(ii) Chief Information Officer
(iii) Chief Executive Officer
(iv) Information Security Committee
(v) Board Integrated Risk Management Committee
(vi) Board of Directors

[c] Whether this incident was reported to:

(i) Sri Lanka Computer Emergency Readiness Team (SLCERT)
(ii) Financial Sector Computer Security Incident Response Team (FinCSIRT)
(iii) Payment and Settlement Department of Central Bank of Sri Lanka
(iv) Computer Crime Investigation Division (CCID)
(v) Any other relevant legal authorities