National Incidents Classification Framework (NISF)

This Framework shall be used by Sri Lanka CERT to determine the severity of the incident at the national level as shown in Figure 1. Based on their impacts, incidents shall be classified into several categories, namely, CAT 1: Critical, CAT 2: High, CAT 3: Moderate, and CAT 4: Minor.

Figure 1: National Incident Classification Framework

Level of Impact	Impact at national or sectorial level, long-term sustain impact (National Cyber Emergency)	CAT 4	CAT 3	CAT 2	CAT 1	CAT 1
	Impact on a specific organization, medium-term impact	CAT 4	CAT 4	CAT 3	CAT 2	CAT 1
	Impact on the specific function of the organization (not to the entire organization), very short-term impact, attempt to breach	CAT 4	CAT 4	CAT 4	CAT 3	CAT 3
National Incidents Classification Framework		**Type 5 Organizations:** Small-scale corporate, Individual	**Type 4 Organizations:** District, Divisional Secretariat, Local Authority, Other government organizations, Large to Mid-size corporate	**Type 3 Organizations:** Central Government Organization (Ministry, Department, Provincial Council, Critical Statutory Board)	**Type 2 Organizations:** President Secretariat, PMO, Parliament, Cabinet Office	**Type 1 Organizations:** Organizations dealing with national security, public health, and safety, foreign relations, banking, and finance, or CNII service providers
		Type of Organization				

The Table below presents a detailed description of the category of incidents that can be used to determine the level of impact.

Table 1: Details of National Incident Classification Framework

CAT 1 Critical	CAT 2 High	CAT 3 Moderate	CAT 4 Minor
Description of Impact o Lead directly to widespread loss of life or directly threaten life. o Nationwide outage of providing essential services by CNII, or serious damage to operations of Type 1 and 2 organizations where serious damage to national security, public health, and safety, foreign relations, and economy. o Nationwide service outage of CNIIs, and no alternative service delivery o A large number of organizations being critically affected o Significant amount of the population is negatively affected. o Resolution to the incident is unknown	Description of Impact o Significantly damage to the operations, and IT assets of Types 2 and 3 organization's functions and leading to the instability of the organization. o Impact at the national and sectoral level, with relatively less critical o Significant impact on reputation o Recovery solution is known, however, would cause significant restoration time. o Breach (or risk of being compromised) of sensitive data of the organization or citizens.	Description of Impact o Moderate level impact on functions of Types 1, 2, 3, and 4 organizations. o No significant damage to national security, foreign relations, economy, banking, finance, or operations of CNIIs. o Less sensitive information being disclosed (or risk of being disclosed). o Service of the disrupted operations can be performed manually. o Restoration can be done in a shorter period.	Description of Impact o Nil or minor effect on the national security, foreign relations, economy, banking, and finance or delivery of CNIIs. o Nil or minor effect on national or sectoral level. o Nil or minor effect on the operations, IT assets of any type of organization, and disrupted functions can be interrupted for extended periods with little or no costs to the organization or individual.

Institutional Incidents Classification Framework (IICF)

The Figure below presents an overview of the Institutional Incidents Classification Framework (IICF). Institutions shall use this classification as a yardstick to assess the criticality of the incidents. Level 1 and 2 incidents may lead to CAT 1 and CAT 2 incidents as defined in the National Incidents Classification Framework (Figure 1) and therefore should report to Sri Lanka CERT in line with the timeliness given in Table 3.

Figure 2: Institutional Incidents Classification Framework

Classification	Details	Possible Attacks
Level 1: Critical	○ Lead directly to the loss of life or directly threaten life. ○ Significant damage to national security, public health, and safety, foreign relations, or economy. ○ Incident affecting CNII of organization and service outage impact nationwide or sectoral level service outage. ○ A large number (50%) of staff is unable to perform the work. ○ Severe reputational damages to the organization	○ Distributed Denial of Service Attack ○ Compromised CNII (internal and external hacking) ○ Spread of virus or ransomware ○ Virus / Worm (outbreak) Destruction of property due to disaster
Level 2: Moderate	○ Incident affecting moderately critical systems or information. ○ No or insignificant impact on national security, economy, foreign relations, public health, and safety. ○ Approximately 25% of staff are unable to perform work. ○ Alternative service delivery is available. However, requires additional staff and resources. ○ Possible breach of non-sensitive data. ○ Incident affecting moderate impact on revenue or customers/citizens. ○ Some reputational damages to the organization.	○ Internal Hacking (not active) ○ Unauthorized access to the noncritical system ○ Unlawful activity. ○ Compromised information.
Level 3: Minor	○ Incident affecting none critical systems or information. ○ Restoration can be in a shorter period. ○ A very few number of staff are affected. ○ No revenue or customer impact. ○ No breach of data ○ No reputational damage to the organization, or economic loss to the organization.	○ Noncritical email/account compromise ○ Inappropriate use of property ○ Policy violations

Reporting Incidents to Sri Lanka CERT

Information and Cyber Security Policy requires government organizations to report critical incidents to Sri Lanka CERT. The timelines for reporting incidents are summarized below.

Table 3: Timelines of Incidents

	Level 1*	Level 2*	Level 3*
Report time to CERT	Immediately (Mandatory reporting)	Within 24 Hour	Not necessary to report
Response time by CERT	Immediately as practical	Within 24 hours as practical	Within 48 to 72 hours as practical
Availability of onsite engineering support by CERT	Yes	No onsite support, advisory support is available	No, online support

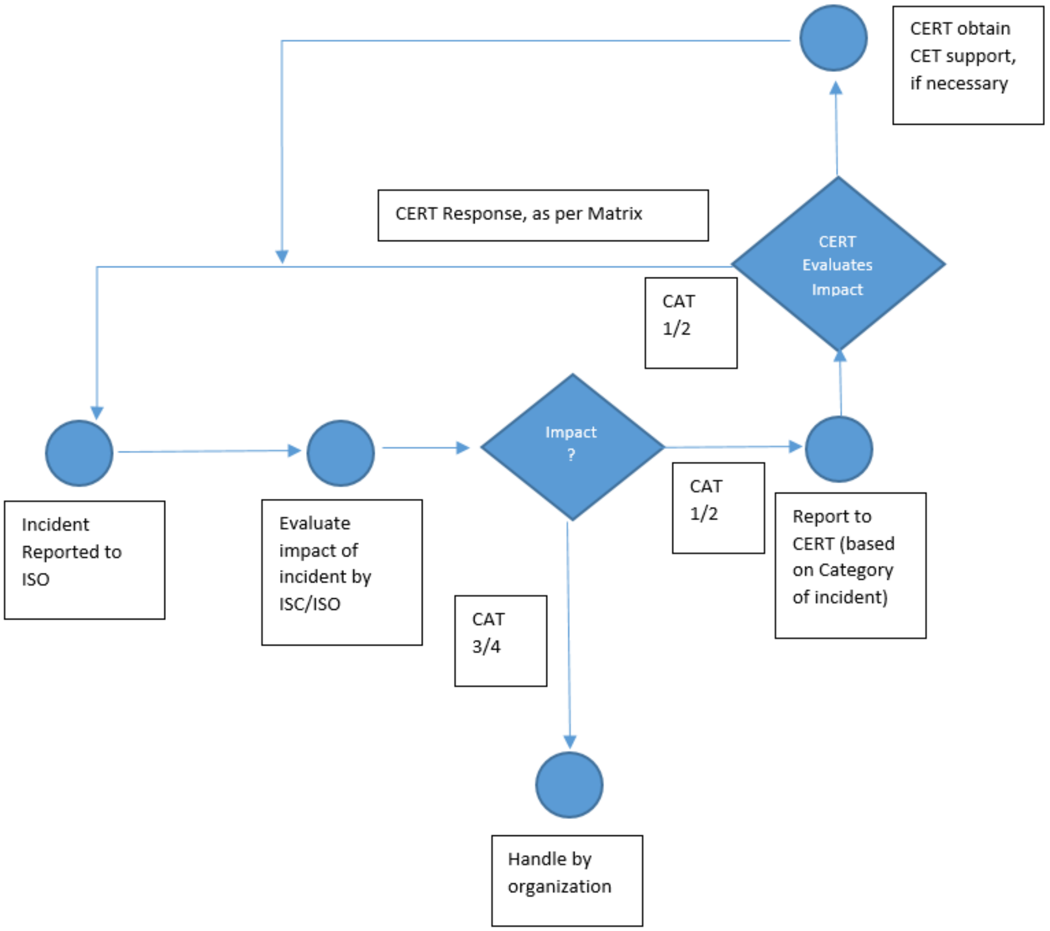
* Levels are defined in the "Institutional Incidents Classification Framework".

Incident Reporting and Handling Process

In the event of an incident, Information Security Committee (ISC) shall first determine the level of the incident based on the Institutional Incidents Classification Framework presented in Figure 2. Information Security Officer (ISO) shall report incidents to Sri Lanka CERT (for CAT 1 & 2) for necessary actions.

Further, all staff shall be advised to immediately report any suspicious activity or any incident to ISO. The organization shall provide adequate awareness and training to staff on the detection of incidents, reporting information security events detected, and preserving evidence. Figure 3 presents an overview of the incident response process.

Figure 3: Incident Response Process


CERT obtain CET support, if necessary
CERT Response, as per Matrix
CERT Evaluates Impact
CAT 1/2
Impact ?
CAT 1/2
Incident Reported to ISO
Evaluate impact of incident by ISC/ISO
CAT 3/4
Report to CERT (based on Category of incident)
Handle by organization