Policy – Information Security Incident Management

Introduction

The GlobalLogic Policy – Information Security Incident Management is documented to provide a well-defined, consistent, and organized approach for managing reported information security incidents, as well as taking appropriate action when an incident at an external organization is traced back to and reported to GlobalLogic.

1. Scope

Any reported Information Security events, incidents, vulnerabilities by any means of communication to the Information Security Team are in scope of the Policy.

2. Roles and Responsibilities

CSIRT - The Cyber Security Incident Response Team led by the Chief Information Security Officer. The mission of CSIRT is to provide an immediate, effective, and skillful response to any unexpected incident with information security implications (i.e., negatively impacting the confidentiality, integrity, or availability of GlobalLogic systems or data). CSIRT is authorized to take appropriate steps to contain and remediate an incident.

Chief Information Officer (CIO) is responsible for giving the CSIRT the highest authority they need to operate, as well as to make the big decisions based on input from the other members of the team. Determines if production services should be taken offline until incident resolution.

Chief Information Security Officer (CISO) provides preparedness resources for CSIRT to respond to security incidents. Coordinates CIRT assignment and response to High-Risk incidents, manages the incident Lessons Learned process.

Head of Security Risk and Compliance is ensuring prompt analysis and evaluation of information security incidents and reporting. Escalates all High-Risk incidents to the CISO.

Information Security Officer (ISO) is responsible for handling, investigating and initial event/incident classification. Collects/preserves pertinent information regarding the incident. Works to contain, remediate, resolve, and document security incidents.

Regional IT Head is managing the IT team at country/region level; responsible for assuring continuity of IT services in particular countries/regions.

Head of IT Infrastructure is responsible for assuring continuity of IT services; supervising team of System Administrators.

Head of IT Network is responsible for assuring continuity of network services; supervising team of Network Administrators.

System/Application owner is responsible for collection and provision of the required evidence to support the handling of the respective incidents and to execute the necessary containment and remediation actions/steps.

Security Operation Center is responsible for consistent monitoring of GlobalLogic infrastructure according to defined scope and job responsibilities.

Incident Reporter provides background information on events which may help understand the cause of an incident in accordance with the **Procedure - Reporting Information Security Events**.

Delivery Project Managers/Directors perform proper reporting of security problems, implement corrective and preventive actions in their areas and support ISO in incident management activity, ensuring required resources are provided and actions are performed without undue delay.

All technical staff and other employees, consultants, contractors or third parties, are required to provide adequate support to the ISO in managing information security incidents.

Abbreviations and Definitions

Abbreviation/ Definitions	Description
Security Incident	A series of unexpected events that involves an attack or series of attacks (compromise and/or breach of security) at one or more sites .A security incident normally includes an estimation of its level of impact. A limited number of impact levels are defined and, for each, the specific actions required and the people who need to be notified are identified.
Cybersecurity Incident	A cybersecurity incident is any unauthorized or malicious activity that compromises the security of information systems, data, or networks. This includes unauthorized access, data breaches, malware infections, denial of service attacks, and other activities threatening the confidentiality, integrity, or availability of company IT assets, as outlined in our Information Security policy
Security Events	Any observable occurrence that is relevant to information security.
Vulnerability	A weak point of the system (in hardware or software) that an intruder could exploit to gain access to system resources for data theft or malicious purposes.
CSIRT	The Cyber Security Incident Response Team
CIO	Chief Information Officer
CISO	Chief Information Security Officer
ISO	Information Security Officer

Description

3. Incident management

For any information security events, incidents, or vulnerabilities, the following steps should be followed:

3.1 Detection:

3.1.1 Potential information security ***events*** or ***incidents*** should be reported immediately to the Information Security Officer (ISO) through Information Security HelpDesk or other means of communication once it is observed or experienced.

3.1.2 ***Vulnerabilities*** discovered in IT Systems are reported by/to the SOC team via Information Security HelpDesk, following principles declared in **Procedure - Vulnerability Management.**

3.1.3 Incident Reporter, if applicable, is responsible to provide detailed information about the reported case.

3.1.4 CISO is responsible for sharing all details about incidents with CIO and General Counsel and provides timely updates on incident containment and remediation.

3.2 Reaction:

3.2.1 Reported cases are assessed by ISO and may be re-categorized based on the gathered details into **event, vulnerability or incident** depending on its nature and impact.

3.2.2 The ISO prioritizes responses based on the criticality of business systems, the risk to information security, and available resources.

3.2.3 Incident impact is determined by the ISO using criteria of Low, Medium, and High.

Low

- Reputation and Customer confidence is not affected.
- One-time financial loss is less than $20.000
- No queries from government or other investigative organizations (or such queries are not foreseeable)

Medium

- Reputation is damaged and some effort and expense is required to recover. Customer relationship is threatened due to loss of confidence
- One-time financial loss is $20.000 - $50.000
- Government or other investigative organizations request information or records (low profile), or such requests are foreseeable.

High

- Reputation is irrevocably destroyed or damaged. Key customer loss
- One-time financial loss is more than $50.000
- Government or other investigative organizations initiate a high-profile, in-depth investigation into organizational practices, or this initiation is foreseeable.

3.2.4 If an incident impacts a project's infrastructure or customer data, the Project Manager and/or Delivery Project Managers/Directors must be informed immediately. They should further inform the client after consultation with Legal and Information Security.

3.3 Containment:

3.3.1 CSIRT in cooperation with involved specialists takes necessary containment and eradication steps. An incident is considered contained when no additional harm can be caused and the incident handler is able to focus on remediation.

3.4 Remediation:

3.4.1 ISO is responsible for determining the incident root cause based on information gathered during the detection phase. Assistance of technical staff, other consultants and/or third parties may be required.

3.4.2 For cybersecurity incidents, actions include comparing affected systems against the original baseline, testing system functionality, restoring the system to the production environment, and performing ongoing system monitoring.

3.4.3 The ISO may involve other departments in the remediation process as necessary.

3.5 Resolution:

3.5.1 During the Resolution phase, the ISO coordinates activities necessary to contain and recover from the incident and implement a contingency plan. ISO confirms the affected business systems are restored before returning to normal working state.

3.6 Closure and Lessons Learned:

3.6.1 Incident handling documentation should be finalized by ISO.

3.6.2 ISO is responsible for closing out the incident.

3.6.3 CISO is responsible for providing reports to external authorities (e.g. client) if required.

3.6.4 Head of HR may be involved for disciplinary action initiation once the root cause of the issue is identified. ISO is responsible for providing all the details to the Head of HR.

3.6.5 **System/Application owners** in cooperation with the Information Security Group are responsible for planning and implementing preventative action to avoid any further recurrence.

3.6.6 ISO is responsible for collecting and securing audit trails and forensic evidence.

3.6.7 In the Closure and Lessons Learned phase, the ISO documents findings from the incident. The expected outcome of this phase is improved operations.

3.6.8 Risk reassessment may be initiated by ISO if required.

3.7 Incident Reporting:

3.7.1 If necessary, an incident report may be provided to other interested parties, depending on the nature of the incident. Incident report should be prepared using approved GlobalLogic template - Information Security Incident Report.

3.7.2 ISO is responsible for preparing an annual report to the CISO which identifies the number, type, category and severity of information security incidents during the preceding period and recommends (where appropriate) additional controls that might limit the frequency of information security incidents, improving GlobalLogic’s ability to respond. This report should be reviewed during Management Review.

3.7.3 All the incident reports from the period since the last management review are considered at the next one, to ensure that GlobalLogic learns from the incidents.

3.7.4 For Personal Data Security Breach please refer to **Information Security Incident Data Breach Procedure** and notification.

3.7.5 Separately, reports in the latest Hitachi format are submitted to the Security Risk Management Division of Hitachi DSS.

4. Escalation Paths

Escalation path for cybersecurity incidents:

1. Head of IT Infrastructure and/or Head of IT Network and/or Head of IT Support and/or Program Director.
2. Country IT Head.
3. Chief Information Security Officer (CISO).

4. Chief Information Officer (CIO).

Escalation path for other Information Security related incidents:

Escalation of non-cybersecurity incidents is regulated within the organizational structure of the impacted department. CISO should be notified. CIO may be involved as a highest escalation point.

Change History

Revision	Change Description	Valid Date	Approver
1.0	Document is created based on Guideline – Cyber Security Incident Response and Guideline – Responding to Information Security Reports	10/20/2020	Alok Malik, CISO
2.0	Guideline was changed to Policy due to documents restructure project. Information Security Department was changed to Information Security Group. Guideline – Reporting Information Security Events in Roles and Responsibilities section was changed to Procedure – Reporting Information Security Events. Guideline – Vulnerability Management was changed to Policy – Vulnerability Management in section 3.1.2	01/25/2021	Alok Malik, CISO
2.0	Annual review - no changes	23/03/2022	Alok Malik, CISO
2.1	Date Format of Valid Date was corrected	03/23/2022	Alok Malik, CISO
2.2	Point 3.7.5 was added to section 3.7	11/18/2022	Alok Malik, CISO
2.3	Cybersecurity incident definition was added to Abbreviations and Definitions	12/15/2023	Denys Kudriavchenko, Head of Security Risk&Compliance