Wipro’s

Logging and Monitoring Policy

**Document Control**

|  |  |
| --- | --- |
| Function | Group Chief Information Security Office (GCISO) |
| Sub-function | - |
| Policy Owner | Lakshminarayanan RS, Group Head - Information Security Policy & Framework |
| Policy Effective Date | March 20, 2019 |

**Purpose**

This policy emphasizes the requirement of logging, monitoring, and analyzing security events to identify and detect any anomalous behavior and potential information security incidents. This policy also specifies identifying threats through the utilization of threat intelligence, threat detection, and threat-hunting techniques.

**Audience**

Organization’s employees, retainers, contractors, and service providers.

**Scope**

This policy applies to all information systems owned or managed by the Organization.

**Policy Details**

**LM.1** Logging, monitoring, and analyzing capabilities shall be implemented as per the applicable laws, regulations, and business requirements.

**LM.2** Security event logs and alerts shall be enabled as per the Logging and Monitoring Standard.

**LM.3** The information systems administrator’s activities shall be logged and monitored with centralized security monitoring tools.

**LM.4** Clock synchronization shall be enabled for Organization’s information systems.

**LM.5** Automated security monitoring tools shall be configured as per business requirements.

**LM.6** Security configuration of known behavior patterns shall be defined and updated.

**LM.7** Near real-time security event log monitoring shall be enabled to identify unusual and anomalous behaviors.

**LM.8** Security event logs shall be protected against unauthorized access, alteration, disclosure, misuse, and destruction.

**LM.9** Personal Identifiable Information (PII) in security event logs shall be masked.

**LM.10** Adequate storage capacity shall be planned for security logs based on business requirements.

**LM.11** Threat hunting and threat detection shall be performed to identify cyber incidents and execute cyber responses.

**LM.12** The Organization shall receive threat intelligence from internal and external sources which shall be considered to identify potential threats, enable monitoring, and take appropriate actions to reduce cyber risks.

**LM.13** Periodic awareness of emerging threats shall be communicated to users.

**LM.14** Security event logs shall be retained as per the Logging and Monitoring Standard.

**Definitions**

|  |  |
| --- | --- |
| **Definition** | **Description** |
| Data Masking | The process of partially or completely replacing sensitive data with random characters or non-sensitive data. |
| Information Security Event | Identified occurrence of a system, service, or network state indicating a possible breach of information security policy, failure of controls, or a previously unknown situation relevant to its security. |
| Information Systems | Set of applications, services, information technology assets, or other information-handling components. |
| Information Security Incident | A single or a series of unwanted or unexpected information security events that create a significant probability of compromising business operations and threaten information security. |
| Threat Detection | The process of monitoring, identifying, and providing alerts on malicious cyberthreat activity. |
| Threat Hunting | A proactive approach to identify previously unknown, or ongoing non-remediated threats within an Organization's network. |
| Threat Intelligence | Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes. |
| Organization | Wipro Limited, including subsidiaries, affiliates, and acquired entities, but excluding acquired entities governed by an independent set of security policies. |
| Personal Identifiable Information (PII) | Data that could potentially identify a specific individual directly or indirectly. It includes but is not limited to, name, date of birth, social security number, government or national identifier, address, telephone number, employee ID number, credit card number, and passwords. |
| Users | The term “User” includes employee of the Organization, retainers, contractors, trainees or interns, customers, partners, suppliers, and vendors. |
| Vulnerability | A weakness in an information system, system security procedures, or internal controls that could be exploited or triggered by a threat source. |

#### Acronyms

|  |  |
| --- | --- |
| **Acronym** | **Description** |
| GCISO | Group Chief Information Security Office |
| PII | Personal Identifiable Information |

**References**

* Security Patch Management Policy
* Data Retention Policy
* Data Protection and Privacy Policy
* Clock Synchronization Standard
* Logging and Monitoring Standard

**Revision History**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Revision Date** | **Reason for Change** | **Drafted/ Reviewed By** | **Approved By** | **Date Approved** |
| 1.0 | 25th July 2023 | Renamed to “Logging and Monitoring Policy” from “Cyber Threat Detection Policy”.  Reviewed and updated the policy as per the ISO 27001:2022 and best practices of NIST 800-53 Rev5. | Roju Vadakkath | Lakshminarayanan RS | 15th January 2024 |