INFORMATION SECURITY INCIDENT MANAGEMENT

Information Technology Department

Document ID	**ITSS-Info-02**
Version Number:	**1.3**
Dated:	**1st October 2024**

1. Policy Statement

IT Support Team will ensure that it reacts appropriately to any actual or suspected events; probably incidents relating to information systems and data.

2. Purpose

The purpose of "Information Security Incident Management" is to mitigate the risks of computer security incidents by providing practical guideline son how to respond to an incident effectively and efficiently. The guidelines are provided to establish an effective incident response program. This document focuses on how to detect, analyse, prioritize, and handle incidents.

3. Scope

This policy and guidelines imply to all employees, students, any 3rd party vendors and contractors which by any means interacts or may interact with organization's Information Security Management System

4. Incident Definition and Classification

- Any event that has a negative effect on the confidentiality, integrity, or availability of an organization's assets.
- An unplanned interruption to an IT Service or a reduction in the quality of an IT Service.
- Any adverse event which compromises some aspect of computer or network security.
- A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

This procedure applies to information security incidents that impact the confidentiality, integrity and availability of information assets:

- Business Processes
- Hardware and network components
- Software
- Applications

- Operating systems
- Databases
- Physical and environmental security components
- Third party services

The following events are classified as Computer/ IT Security Incidents:

- Loss of Service, equipment or facilities
- Non-compliance with policies or guidelines
- Malfunctions of software or hardware
- Any attempted network intrusion
- Any attempted denial-of-service attack
- Any detection of malicious software
- Any unauthorized access of data
- Any violation of security policies including acceptable usage policy
- Power failure which may cause unavailability of Data Center Services
- Cooling System failure which may cause unavailability of Data Center Services
- 3rd Party Data/ Internet circuit disruption
- Lost or Theft of equipment
- Intentional or Unintentional damage to physical infrastructure
- Any other event that might interrupt Confidentiality, Availability and Integrity of data and information system

4.1. Events and Incidents:

4.1.1. Events

Any change of state that has significance for the management of IT services. Events can be normal (e.g., a user logs in) or abnormal (e.g., a server goes offline).

4.1.2. Incident

An unplanned interruption to IT services OR a reduction in the quality of an IT service. Incidents may be detected through events.

4.2. Incident Detection Mechanisms

4.2.1. Automated Monitoring

Use of tools for continuous monitoring IT services and Infrastructure and identify deviations from normal operations.

4.2.2. Threshold-Based Alerts

Notifications triggered when specific metrics exceed predefined limits.

4.2.3. Synthetic Transactions

Simulated user activities to test and monitor the performance of applications.

4.2.4. Event Correlation

Event correlation is the analysis of different events for pattern identification which may indicate a more severe problem.

4.2.5. SIEM (Security Information and Event Management)

Systems that collect analyze and report on security-related data from across the IT environment.

5. Detection Mechanisms

5.1. Automated Monitoring Systems

- Implement continuous monitoring for all critical IT services, infrastructure components, and networks.
- Utilize tools like PRTG, MRTG, and Observium for real-time monitoring of performance, bandwidth, and service availability.
- Deploy Application Performance Monitoring (APM) tools such as SigNoz and Graphite to track application performance and detect anomalies.

5.2. Log Management

- Centralize the collection and analysis of log data from all relevant systems, including servers, applications, and network devices.
- Implement tools like the ELK Stack (Elasticsearch, Logstash, Kibana) to detect error messages, failed login attempts, and other significant events.

5.3. Threshold-Based Alerts:

- Establish and document thresholds for key performance indicators (KPIs) like CPU usage, memory utilization, and response times.
- Set up automated alerts to notify the IT team when these thresholds are breached, ensuring immediate attention to potential issues.

5.4. Synthetic Transactions:

- Utilize synthetic transactions to simulate user interactions with critical applications and services.
- Regularly schedule these transactions to detect performance issues proactively, using tools like Selenium or Uptime Robot.

5.5. Event Correlation:

- Employ event correlation engines to analyses events from multiple sources and identify patterns that could signify broader issues.
- Correlate events to reduce noise and focus on high-impact events, using tools such as Moog soft or GrayLog.

5.6. Security Information and Event Management (SIEM):

- Integrate SIEM systems like Security Onion or OSSIM to centralize the collection and analysis of security-related data.
- Enable real-time detection and response to security threats by continuously monitoring and analyzing data from firewalls, IDS/IPS, and other security tools.

6. Integration with Incident Management

6.1. Event Escalation:

- Define criteria for escalating events to incidents based on their severity, impact, and urgency.
- Ensure seamless integration with the Incident Management process for prompt and effective response.

6.2. CMDB Integration:

- Integrate detection mechanisms with the Configuration Management Database (CMDB) to assess the impact of detected events on related services and assets.
- Use the CMDB to prioritize incident response based on the criticality of affected components.

7. Compliance with ISO 27001

7.1. Information Security Considerations

- Ensure that all detection mechanisms are aligned with ISO 27001 controls, particularly A.12.4 (Logging and monitoring) and A.16 (Information security incident management).

- Maintain comprehensive logs and records of all detected events, including their nature, time of detection, actions taken, and outcomes.

7.2. Documentation and Record-Keeping

- Keep detailed documentation of all events and incidents in accordance with ISO 27001 requirements.

- Ensure that records are securely stored and accessible only to authorized personnel.

7.3. Regular Reviews and Audits

- Schedule regular reviews of detection mechanisms to ensure they remain effective and compliant with ISO 27001 standards.

- Conduct periodic audits to verify the functionality and alignment of monitoring processes with established policies.

8. Continuous Improvement

8.1. Feedback Loops:

- Implement feedback mechanisms to capture lessons learned from detected events and incidents. For all the incidents a n incident report is generated with all necessary information and steps taken for the triage. This also contains the steps to ensure that the reoccurrence of the incident should be minimize.

- Regularly review and refine detection mechanisms based on feedback and evolving best practices.

8.2. Training and Awareness:

- Provide ongoing training for IT staff on the use of detection tools, processes, and best practices.

- Promote awareness of the importance of timely event detection and reporting to maintain IT service quality and security.

9. Incident Severity and Impact Assessment

9.1. Classification:

Incidents must be classified by severity (High, Medium, Low) and impact (Business Impact, Service Impact, User Impact) to determine the appropriate escalation path.

9.1.1. Incident Classification

Incidents should be classified based on their Severity, Impact, Type, Source, and Urgency, in line with ITIL best practices and ISO 27001 requirements.

9.1.1.1. Severity Levels

9.1.1.1.1. High Severity:

- Critical systems are down, posing a significant threat to business operations.

- Immediate action is required to prevent significant loss or impact.
- Quantifiable thresholds should be established, such as downtime exceeding a specific duration or affecting a defined percentage of users.

9.1.1.1.2. Medium Severity

- Non-critical systems are affected.
- Action is required, but there is no immediate business threat.

9.1.1.1.3. Low Severity

- Minor issues with minimal impact on business operations.
- Can be addressed during regular business hours.

9.1.1.2. Impact Levels

9.1.1.2.1. Business Impact

- Affects critical business operations, resulting in revenue loss or significant operational disruption.

9.1.1.2.2. Service Impact:

- Affects one or more IT services but may not directly affect business operations.

9.1.1.2.3. User Impact:

- Affects end-users, such as staff or customers, but does not directly affect core business functions.

9.1.1.2.4. Information Security Impact:

- Affects the confidentiality, integrity, or availability of information, potentially

leading to compliance issues or data breaches.

10. Incident Response Lifecycle

Incident management is an ongoing activity and the results of post-incident recovery are used to improve detection methods and help in preventing a repeated incident. The Incident Response Lifecycle for Iqra University encompasses of following steps:

10.1. Detection

An incident can be detected by the following ways:

- Alerts generated by IPS/ IDS and Firewalls.
- Real Time event correlation
- Malware detected by endpoint
- System audit logs
- Events detected by End users and IT Staff
- Complaints from end users.

10.2. Response

If the event detected in the first step is classified as an incident, the following steps will be taken depending on the criticality of the incident:

For Minor incidents refer to the **"IT Support Escalation Matrix"**

10.2.1. Computer Security Incident Response Team (CSIRT)

For major security incidents, CSIRT will be activated through the instructions of Director Digital Transformation. The following are the conditions for activation of CSIRT:

- Any major data breach
- An ongoing attack
- Any disruption to critical services which includes LMS, Financial Applications, Database Services and Web Services.

- Any incident that may bring down partially or completely any service at Iqra University

10.2.2. Computer Security Incident Response Team (CSIRT) Members

Following are the members of CSIRT

10.2.2.1. Major Incident Management:

- Team: IT Service Management Team
- Contact: Rizwan Anwar,
- Phone : 9803,
- Email : rizwan@iqra.edu.pk

Responsibilities:

- Manage Complex and Critical Incidents escalated from L2/ Event Management.
- Coordinate with external vendors or higher management.

- Team: IT Service Management Team
- Contact: Danish Akhlaq,
- Phone: 9840
- Email: danish.akhlaq@iqra.edu.pk

Responsibilities:

- Manage Complex and Critical Incidents escalated from L2/ Event Management.
- Coordinate with external vendors or higher management.

- Team: IT Service Management Team
- Contact: Yasir Ahmed,
- Phone: 9802
- Email: yasir.ahmed@iqra.edu.pk

Responsibilities:

- Manage Complex and Critical Incidents escalated from L2 and L3.
- Coordinate with external vendors or higher management.

- Team: DLIC
- Contact: Iftikhar Ahmed,
- Phone: 9804
- Email: Iftikhar.ahmed@iqra.edu.pk

Responsibilities:

- Manage LMS, Employee Support Service and ODOO
- Coordinate with external vendors or higher management.

10.2.2.2. Executive Decision & Resolution:

- Team: Director Digital Transformation
- Contact: Moneeb Khan,
- Phone: 9801,
- Email : dir.dt@iqra.edu.pk

Responsibilities:

- Final escalation points for unresolved critical incidents.
- Make strategic decisions for major service disruptions.

10.3. Mitigation

During this phase, IT Support or CSIRT will attempt to contain the security incident. Depending on the type of incident, actions performed by IT Support or CSIRT will vary. Detailed notes about the incident will be documented and the chain of custody will be maintained if information technology assets are involved in the incident. This information can be used for digital forensic analysis and can be used during civil and criminal litigation and/or disciplinary/termination action if required.

10.4. Reporting

If an incident occurred report of the incident will be provided to upper management depending upon the nature of the incident.

In compliance with regulations incident reports will be shared with external parties if required.

If a data breach exposes Personal Identifiable information, the user will be notified as regulated by the law.

The following might also be notified depending on the nature of the incident:

- Vice Chancellor
- Director Digital Transformation
- Department Heads
- Local information security officer
- Other incident response teams within the organization
- External incident response teams (if appropriate)
- System owner
- Human resources (for cases involving employees, such as harassment through email)
- Public affairs (for incidents that may generate publicity)
- Legal department (for incidents with potential legal ramifications)
- Law enforcement (if appropriate)

10.5. Remediation

Root cause analysis of incident will be done in cooperation with CSIRT to determine what caused the incident to occur.

Methods and Controls will be established depending on the Root Cause Analysis to prevent the recurrence of the incident.

10.6. Lessons Learned

"Lessons learned" meeting with all involved parties after a major incident, and periodically after lesser incidents should be held providing a chance to achieve closure with respect to an incident by reviewing what occurred, what was done to intervene, and how well intervention worked.

The following questions will be asked in the meeting:

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

11. Incident Attack Vectors and Classification Criteria

The attack vectors listed below the list common methods of attacks on the basis of which the incident classification scheme is defined.

11.1. External/Removable Media:

An attack executed from removable media or a peripheral device, for example, malicious code spreading onto a system from an infected USB flash drive.

11.2. Attrition:

An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services (e.g., a DDoS intended to impair or deny access to a service or application; a brute force attack against an authentication mechanism, such as passwords, CAPTCHAS, or digital signatures).

11.3. Web:

An attack executed from a website or web-based application—for example, a cross-site scripting attack used to steal credentials or a redirect to a site that exploits browser vulnerability and installs malware.

11.4. Email:

An attack executed via an email message or attachment for example, exploit code disguised as an attached document or a link to a malicious website in the body of an email message.

11.5. Impersonation:

An attack involving the replacement of something benign with something malicious— for example, spoofing, man-in-the-middle attacks, rogue wireless access points, and SQL injection attacks all involve impersonation.

11.6. Improper Usage:

Any incident resulting from the violation of an organization's acceptable usage policies by an authorized user, excluding the above categories; for example, a user installs file sharing software, leading to the loss of sensitive data; or a user performing illegal activities on a system

11.7. Loss or Theft of Equipment:

The loss or theft of a computing device or media used by the organization: such as a laptop, smartphone, or authentication token.

11.8. Other:

Any other attack that does not fit into any of these categories

12. Incident Detection and Analysis Check List

Incident response can be stressful, especially when the incident is severe and business operations are disrupted. Having a robust incident response plan ready before an incident can help organizations quickly and more effectively contain threats and recover, instead of only reacting when the incident happens and trying to make plans on the fly. An incident response plan which has been thought through and rehearsed beforehand is key to containing the incident and limiting damage and disruption to business operations.

This Incident Response Checklist is structured around the IPDRR (Identify, Protect, Detect, Response, and Recover) framework

S#	Action	Remarks
	Detection and Analysis	
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
4	Acquire, preserve, secure, and document evidence	
5	Contain the incident	
6	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered, repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	

	Post-Incident Activity	
8	Create a follow-up report	
9	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	