POLICY NUMBER 2

ITS SERVICE DESK INCIDENT MANAGEMENT

Prepared by	IT Services Division
Approving Authority:	FNU Council
Date Approved:	1 August 2025
Next Review:	1 August 2026
Version Number:	1

1.0 Purpose

The purpose of this ITS Service Desk Incident Management Policy is to establish a standardized process for managing all reported IT-related faults and issues to ensure their timely and effective resolution. Its goal is to minimize operational disruptions, enhance service quality, and improve user satisfaction. By using a consistent approach and the IT Service Desk ticketing system, the policy ensures optimal service availability and reduced business interruptions.

2.0 Policy Scope

This policy applies to all IT staff and users across the organization. It encompasses the identification, classification, management, and resolution of incidents and problems affecting IT services. This includes all incidents reported to the IT Service Desk, such as those related to hardware, software, network, and security. The policy ensures that all incidents are managed through the IT Service Desk ticketing system to provide consistent and efficient handling of issues.

3.0 Definitions

3.1 **Incident:** It refers to any event that disrupts or reduces the quality of an IT service. This includes any IT-related issues such as system failures, software bugs, hardware faults, performance issues, and any other deviation from normal operations.

3.2 **Incident Management:** It is the key process within the IT Service Desk framework, focused on handling and resolving IT service disruptions (faults/issues).

3.3 **IT Service Desk:** The Division of IT Services primary point of contact for all users, providing IT assistance and support ensuring issues and incidents are managed efficiently

3.4 **Priority Levels:** Categories used to define the urgency and impact of an incident.

3.5 **Critical:** Major disruption affecting all FNU users or critical systems essential to university-wide operations. E.g. Banner & Moodle system outage, Internet Outage or Network failure across multiple campuses.

3.6 **High:** Disruption affecting a single campus with significant number of users or essential IT systems. This includes Staff and Student account access.

3.7 **Medium:** Issues affecting a building/ block with limited number of users or non-essential IT systems and services.

3.8 **Low:** Less disruptions with little to no operations impact. Often involving single user issues with available workarounds.

3.9 **Minor:** Minor disruptions and IT schedule tasks.

4.0 Roles & Responsibilities

4.1 Users

4.1.1 Reporting all IT related incidents/problems to the IT Service Desk promptly.

4.1.2 Providing relevant information prior, during and while working with IT staff to resolve the issue.

4.1.3 Must be present on site/at the workstation when the IT Staff is attending the issue in person or remotely.

4.2 IT Service Desk Staff

4.2.1 Logging, categorizing, and prioritizing of all incoming IT issues.

4.2.2 Assigning incidents to the relevant teams for resolution.

4.2.3 Monitoring the progress of incidents and ensuring communication with users.

4.2.4 Providing first-level support and resolving incidents where possible.

4.2.5 Escalate unresolved issues to appropriate second or third-level support staff.

4.3 IT Managers, IT Leaders and IT Service Desk Coordinator

4.3.1 Responsible for overseeing the incident management process.
4.3.2 Identify opportunities for process improvements and participate in reviews or audits of the incident management framework to enhance performance and efficiency.
4.3.3 Escalating incidents that exceed agreed resolution times.
4.3.4 Ensuring root cause analysis for recurring issues
4.3.5 Identify patterns in incidents that may lead to more efficient handling or the development of preventive measures.
4.3.6 Reassigning Incidents to appropriate IT Staff.

4.4 IT Staff and IT Technicians

4.4.1 Handling and resolving incidents assigned by the IT Service Desk.
4.4.2 Ensuring that incidents are resolved within the stipulated time frame based on priority levels.
4.4.3 Provide timely updates to users regarding the status of their incidents, ensuring transparency and managing user expectations.
4.4.4 Notify users when incidents are resolved and confirm that services have been restored before closing the ticket.
4.4.5 Document resolutions for incidents and update the knowledge base to help improve the speed and accuracy of future incident resolutions.

5.0 Policy Principles

5.1 Incident Reporting & Logging

5.1.1 All IT related incidents and problems must be reported and logged in the IT Service Desk ticketing system.
5.1.2 Users must report all incidents via the following channels: (appropriate channels)
Phone: 3381044 Ext 1205
Email: itservicedesk@fnu.ac.fj
5.1.3 The IT Service Desk will log all reported incidents in the IT Ticketing System, assigning a unique reference number to each ticket for tracking purposes.

5.2 Incident Categorization and Prioritization

5.2.1 All IT Problems and Incidents will be categorized according to the affected service and nature of the issue.
5.2.2 All IT related issues, problems and incidents will be prioritized based on the impact and urgency, following the guidelines set in the priority levels.

5.3 Escalation

5.3.1 The IT Service Desk will ensure that unresolved incidents are escalated to the next level based on defined timeframes or priority level as assigned.

5.4 Communication

5.4.1 Users will be regularly updated on the progress of their pending reported IT incident or problem.
5.4.2 Upon resolution, the IT Staff assigned will notify the user accordingly, before any issues is closed in the IT Ticketing System.

5.5 Closure

5.5.1 Incidents or problems should only be closed within the ticketing system once the issue has been resolved, and the user is notified and confirms the resolution.
5.5.2 If no response is received from the user within 8 working hours of resolution, the

incident will be closed.

5.6 Monitoring and Reporting:

5.6.1 Incident and problem metrics (e.g., number of incidents, resolution times, etc.) should be monitored and reported to relevant stakeholders using the reporting features of the ticketing system.

5.6.2 A monthly report will be generated detailing the number of incidents, resolution times, escalations, and trends to ensure continuous improvement.

5.6.3 Regular incident or problem trend analysis should be conducted using data from the ticketing system to identify patterns and prevent future occurrences.

5.6.4 The IT Managers will review incident metrics regularly to track the performance of the incident management process.

6.0 Compliance and Enforcement

Failure to adhere to this policy may result in disciplinary action for IT staff and users, depending on the severity of the non-compliance.