Services Management Policy

Guidebook

Version 1.3

Table of Contents

ISO/IEC 20000-1:2018 is an international standard for Information Technology Service Management (Service Management System: SMS) that provides requirements and best practices for delivering excellent services to customers and internal service recipients within the organization. It outlines the requirements for managing IT service delivery to meet business needs through the ongoing improvement of processes and the continuous enhancement of personnel capabilities, based on data obtained from regular quality monitoring and service evaluations.

Roles of Stakeholders

Internal Stakeholders

Management:

Establish the direction and policies for IT service management, with responsibility for resource allocation and management of associated risks.

The senior management team consists of

- Chief Executive Officer (CEO)
  - Chief Technology Officer (CTO)
  - Chief Operation Officer (COO)

Service Management Representative (SMR): The individual responsible for overseeing the ISO/IEC 20000-1: 2018 standard plays a crucial role in service management by acting as a liaison between the service team and relevant departments. This ensures that service operations are carried out efficiently. Their responsibilities include monitoring to management to inform decisions regarding future developments in service processes. service quality, evaluating performance against established standards, addressing and managing user complaints, promoting continuous improvement in service processes, and supporting team training to ensure everyone understands the relevant policies and procedures. Additionally, they report service operation data and trends

Service Desk/HelpDesk: Responsible for receiving requests and incidents, ensuring that request tickets are tracked and processed in accordance with service level agreements.

Service IT Support:

Responsible for overseeing the information technology systems at the main office and backup office, providing support for the organization's internal computer center.

Service Owner: Service owner in scope, currently encompassing 8 services, will be evaluated based on internal audit requests and the requests for certification of ISO/IEC 20000-1:2018.

Sales: Coordinator between service owners and external customers, responsible for gathering customer requirements and assessing customer satisfaction with the services provided.

CFO (Finance, Purchasing, and Accounting): Responsible for managing the budget, accounting for assets used in service delivery, and tracking the status of those assets.

People Excellence (PE): Responsible for staffing levels, personnel qualifications, knowledge management administration, operational support work, and staff development for knowledge and personnel replacement.

Legal: Oversee and provide advice on legal matters related to information technology, reviewing contracts, licenses used in business operations, and other relevant laws.

Internal Auditor: Responsible for monitoring the implementation of ISO/IEC 27001:2022, ISO/IEC 20000-1:2018, and other standards that the company must adhere to.

Service Users Internal :
Individuals who use IT services within the organization and are important for providing feedback on the quality and satisfaction of the services received.

Service Management System Committee (SMS Committee): Establish policies and strategies for service management, promoting the operations of the SMS Working Team to ensure that service management is effective and aligns with the ISO/IEC 20000-1:2018 standard.

SMS Working Team: The ISO/IEC 20000-1:2018 standard working team manages service operations. Currently, there are 8 services within the scope, consisting of: IT Support, HelpDesk, System Infrastructure, Cybersecurity Operation Center and Management Security (CSOC), Information Security (Infosec), Network and Cisco Customer Experience, IT Operation Managed Services (ITOMS), Infrastructure Services Excellence (ISE)

Document Control Officer (DCO): Responsible for creating, managing, and controlling documents related to the service management system in compliance with ISO/IEC 20000-1:2018, ensuring accessibility, accuracy, security, and compliance with relevant standards.

Audit Working Team: Responsible for conducting internal audits of the service management system in accordance with ISO/IEC 20000-1:2018, assessing compliance and effectiveness, and providing reports and recommendations for continuous improvement.

Knowledge Management Working Team: Responsible for developing and reviewing learning strategies for knowledge management within the organization, while monitoring the effectiveness of usage and maintaining valuable knowledge repositories.

Incident Management Working Team: Responsible for reviewing and assessing the process of incident resolution, including monitoring corrective actions to ensure compliance with service level agreements, analyzing root causes, and assigning corrective measures to relevant departments, while also managing knowledge from incidents to enhance the knowledge management system.

Problem Management Working Team: Evaluate and review the problem-solving process, identify root causes to reduce recurring issues, analyze problems, and assign relevant departments to implement corrective actions. Additionally, manage the knowledge generated from problem-solving activities within the knowledge management system.

Supplier Management Working Team: Manage internal and external vendors and stakeholders, by creating and monitoring clear agreements with external service providers, while continuously evaluating and reporting on the efficiency of the services provided.

Emergency CAB (ECAB): Empowered to review and approve urgent changes, with the ability to authorize changes without requiring approval from the Change Advisory Board (CAB), by assessing whether the details of the change request are appropriate in the change request form.

Change Advisory Board (CAB): Responsible for reviewing and approving urgent (Emergency) changes and standard (Normal) change requests that impact the business, categorizing them into minor and major levels of importance. Review and close out reports collaboratively with the change requestors and change managers to analyze trends and enhance the efficiency of the change processes. Also responsible for other tasks as assigned by the Emergency Change Advisory Board (ECAB).

Information Security Management Representative (ISMR): To oversee and promote compliance with the information security policies within the organization, including coordinating between various departments to ensure that operations are carried out according to established standards and guidelines. Additionally, the role involves reporting the status and issues related to information security to management.

Information Security Management System (ISMS): The development of a framework that enables the organization to systematically manage information security, aimed at identifying, controlling, and reducing risks associated with data. This includes continuous assessment and improvement of processes to achieve certification for information security standards by complying with the requirements and guidelines outlined in ISO/IEC 27001:2022, creating an information security management system that aligns with the CIA concept.

CIA stands for »

Confidentiality: This involves controlling access to information to ensure that unauthorized individuals cannot access it.

Integrity: This refers to maintaining the accuracy and completeness of information, ensuring that it is suitable for use and has not been altered or tampered with without authorization.

Availability: This means that information should always be readily available for those who are authorized to access it.

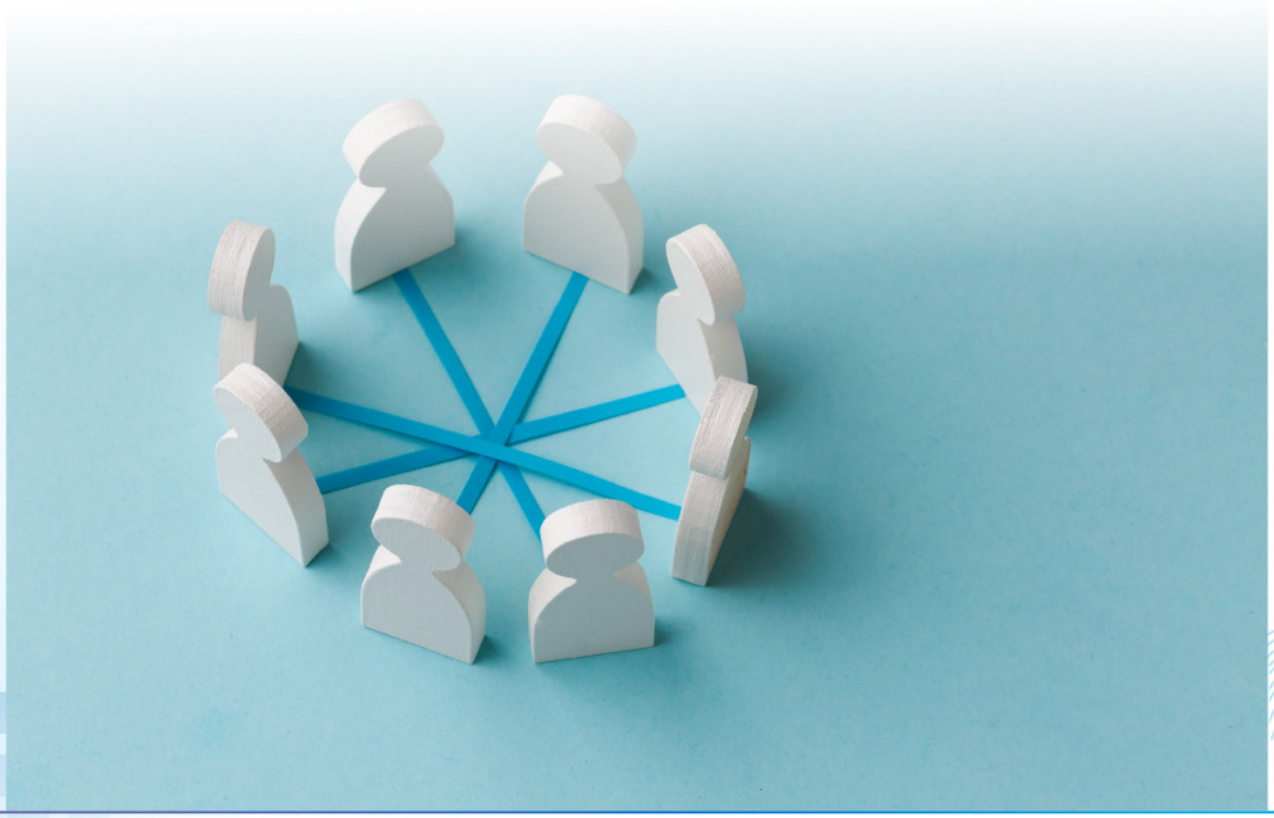
IT Governance : The Information Technology Working Group is responsible for various operations of the information technology systems, including the management of information security systems.

ISMS Working Team : The ISO/IEC 27001:2022 Standard Working Team currently has 3 services within its scope, consisting of IT Support, Cybersecurity Operation Center and Management Security (CSOC), and Digital Security Unified Services (DSUS), which work in collaboration with the SMS Working Team.

Roles of Stakeholders

External stakeholders of the organization

Customers: Customers and service users who utilize the services across the entire scope, which impacts the development of services and the improvement of service processes.
Regulatory Bodies: These entities set standards and regulations that the organization must comply with, affecting the operations of IT services, such as data protection laws.
External Service Providers: Individuals or organizations outside that provide services, products, or resources to the company or organization, supporting the operation or the delivery of services effectively to customers.
Business Partners: Organizations may collaborate with business partners, such as service contracts or supply chain management, which contribute to the delivery of IT services.
Investors: Investors play a role in providing financial support and expect returns on their investments, showing interest in the management of services and the benefits the organization can generate.
Competitors: Competitors can influence the policies and strategies of the organization's service management, which impacts customer expectations and decision-making.



1

Service Management Objective

Business

1. Implementation of service work to meet business needs. And according to the service level agreement with the user.

Process

2. Efficient Process Development Continuous improvement and compliance with the standard.

Policy/Legal

3. The operation is in line with the organization's directions, policies, and regulations. Company requirements and related laws.

Human

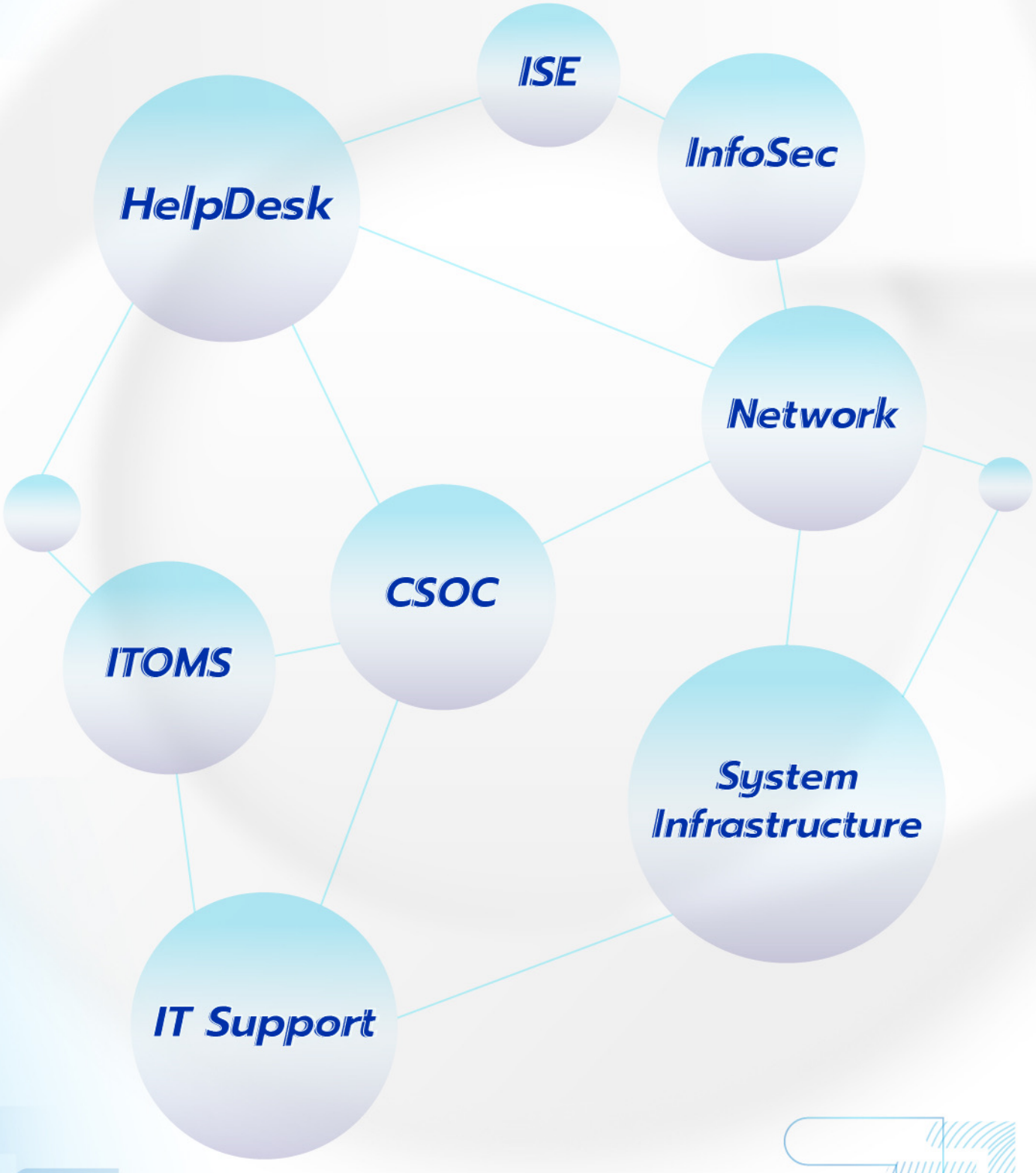
4. Develop personnel to have the knowledge and ability to respond to the company's service work and the needs of service users.

Innovation

5. Bringing innovation to help develop services to be efficient and suitable for the needs of the organization and service users.

2

Service in the Scope



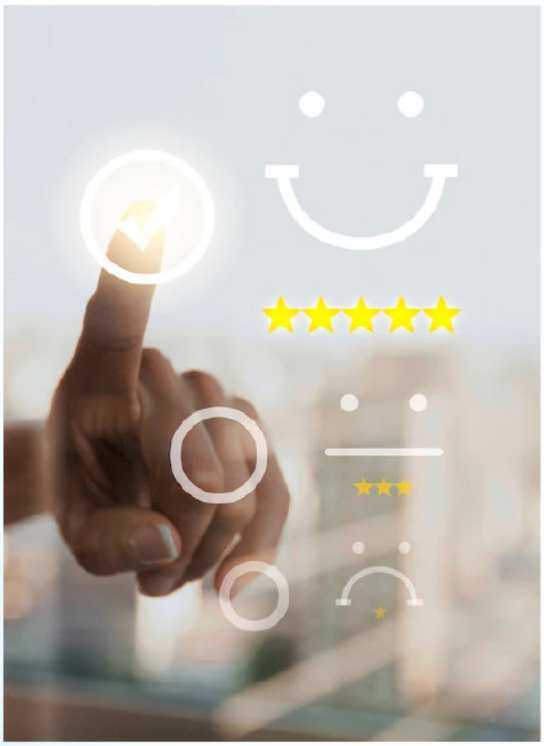
3

Service Management Policy

There are 9 categories as follows

Category 1: Service Management Policy (SM Policy)
Category 2: Budgeting and Accounting Management Policy
Category 3: Service Configuration Management Policy
Category 4: Change Management Policy
Category 5: Release and Deployment Management Policy
Category 6: Incident Management Policy
Category 7: Problem Management Policy
Category 8: Business Continuity Management Policy
Category 9: Information Security Management Policy

Category 1: Service Management Policy (SM Policy)



In the operation of the company's services, it is necessary to establish procedures by specifying the objectives of the Service Management system, SMS Performance Evaluation, SM Policy and SMS Manual which is approved by SMS Committee. For details of the service management policy of the company, it will be related to employees using the service, service managers, individuals involved in supporting both internal and external service operations. The details are as follows:

1. Develop the quality of service to be efficient in responding to customer satisfaction and the business operation direction.
2. Establish work processes and define roles and responsibilities for providing services to ensure that service recipients receive services according to specified agreements.
3. Manage personnel within both internal and external organizations to provide quality service to service recipients.
4. Support resources and tools that facilitate the operation of quality services and can reduce errors in the execution process.
5. Conduct service operations in compliance with laws, regulations, rules, and policies related to service management.

Category 2: Budgeting and Accounting Management Policy

This involves managing the value and cost-effectiveness of service delivery within the service system and the support system for service provision. It is considered crucial to ensure that the company benefits in its operations to achieve business goals. This policy is related to service owners and personnel supporting service operations, with details as follows:

1. Budget management and service accounting operations must be carried out within the scope to align with the business requirements of MFEC PUBLIC COMPANY LIMITED
2. Budget management and service accounting operations within the scope must include specifying job details, work plans, operational guidelines, and the budget set to be sufficient for the service recipients' needs.
3. Investment in budget management processes and service expenses within the scope must support the needs of service recipients.

Category 3: Service Configuration Management Policy

This category deals with the control of service components (Configuration) that impact service delivery within the scope. This policy is related to service owners and personnel supporting service operations, with details as follows:

1. CI (Configuration Item) information must be categorized and assigned unique identification names.
2. Changes to CI data must be carried out through the Change Management Process.
3. Owners are designated for each CI item to oversee responsibility for accuracy and completeness.
4. Configuration Items Audit must be conducted at least once per year.

Category 4: Change Management Policy

Every change that occurs must adhere to the Change Management Procedure to control the components of the service delivery in line with business objectives and mitigate the impact of ineffective changes. This category's policies will be related to service owners and personnel supporting service operations. The details are as follows:

The identification of change types comprises a total of 4 types, namely:

1) Emergency Change
2) Major Change
3) Minor Change
4) Standard Change

Each must be processed following the appropriate steps.

1) Develop a process/procedure for managing Emergency Changes in the event of an emergency, clearly outlined in writing.
2) Establish criteria for determining the urgency of changes to be used in considering the prioritization and execution of change activities.
3) Designate authorities for approving changes of each type, aligned with the operational procedures.
4) All external service providers delivering services must follow the Change Management Procedure steps.
5) Change requests must be analysed to identify continuous improvement opportunities in service management, at least once per year.
6) The Standard Change List is reviewed at least once per year.

Category 5: Release and Deployment Management Policy

This is a method for specifying the procedure to control service changes related to software development or services associated with creating packages before implementing changes. This policy is relevant to service owners and personnel supporting service operations, with details as follows:

1. All Release and Deployment Management activities must be managed and controlled under the Change Management Procedure.
2. The Release Package set to be used in the actual system must undergo installation, testing, verification, and have a Back-out Plan that can be used in case of installation issues.
3. There must be grouping by type and frequency of releases to separate types of releases and determine the frequency at which they will occur.

Category 6: Incident Management Policy

This involves defining the procedure for managing service disruption incident requests to ensure service restoration with minimal impact on the business. This policy is relevant to the Helpdesk team, service recipients, service owners, and personnel supporting service operations. The details are as follows:

1. All incidents must be recorded by the Helpdesk unit to capture information about incidents and historical data. This information will be used for analysis and to derive solutions for problem resolution.
2. Service recipients and all personnel have the responsibility to report incidents to the relevant unit as follows:
   A. The IT Support unit is responsible for incidents that occur internally.
   B. The Helpdesk unit is responsible for incidents that occur externally.
   C. The CSOC unit is responsible for monitoring events from the surveillance system and reporting results from the Dashboard screen to respond to incidents. They also report incidents into the Helpdesk system.
   D. The Hotline system is utilized for issues with CSOC services. Once resolved, notifications are sent to be recorded in the Helpdesk system.
3. Classify incidents based on impact level, urgency, priority, service/system/product type, information security, incident handling team, and incident reporter. This classification is used for reporting and forwarding to relevant processes within information technology services based on incident type, priority level, service recipient, and interactions with various processes.
4. Staff assigned to resolve incidents must understand the escalation rules, response and resolution timeframes, and adhere to the established escalation criteria.
5. The importance level of incidents is divided into 4 levels, namely Critical, High, Medium, and Low. Each level has a specified time frame for resolution according to the company's service agreement.
6. If an incident occurs more than 3 times per week, it should be escalated to a problem resolution request.
7. Incidents will be closed once the incident can be resolved, and services return to normal, with approval from the customer or feedback from the Incident Response Manager.
8. Information or anything provided to service recipients must be recorded and kept current for future service improvement analysis.

Category 7: Problem Management Policy

This is to address the root cause of the problem, aiming to prevent the recurrence of incidents and ensure they do not happen again. The details are as follows:

1. All problems must be documented by the Problem Manager to compile information about the problem and past resolution data. This aids in analysis and finding efficient solutions for problem resolution.
2. The initiation of a problem resolution request can be done either from an incident request or proactively by considering responsibility from the Proactive Problem perspective.
3. The problem resolution request code received from an incident request must specify the linkage with the problem request code. When closing the problem request, ensure the corresponding incident request is appropriately closed.
4. Generate reports on problem resolutions to track progress appropriately.
5. Incidents recurring beyond acceptable thresholds, as determined by the problem management process, must be considered for analysis to identify the root causes of the problem.
6. Resolved problems must be documented with corrective action guidelines, and this information should be utilized in knowledge management processes to address inquiries or searches through the Helpdesk. In cases where improvements or changes are necessary, linkages should be established with the Change Management process.

Category 8: Business Continuity Management Policy

This addresses the provision of services that instils confidence in service recipients that the service system can operate continuously, even in unforeseen circumstances. This policy is relevant to service owners and personnel supporting service operations. Additionally, it complements the Information Security Policy under Section 5, specifically addressing the continuity management of information technology systems. Further details are as follows:

1. Risks or incidents that may impact service interruptions are identified.
2. Continuity plans must be established to support the seamless return to normal operations. Critical service processes should be periodically tested for consistency.
3. Testing continuity plans must include the documentation of achieved and unmet objectives, serving as a basis for continuous improvement in future iterations of the operational procedures.

Category 9: Information Security Management Policy

It is a policy that deals with information security which is considered important in providing services and responding to the protection of data by the company storage and operations to comply with laws related to information technology. In this case, the company refers to its Information Technology Policy (IT Policy).

4

Service Catalogue

Service Name	Helpdesk
Standard Service Features	• Management of system administrator privileges (Service). • Addition/Modification/Deletion of registered components in the system. • Addition/Modification/Deletion of data in Master Data. • Handling and tracking of incident reports from customers until resolution Receiving service requests from customers (Standby, Consult, Install, Report, Others).
Service Hours	24x7 (Day Shift 09:00 AM - 09:00 PM, Night Shift 09:00 PM - 09:00 AM)
Service Requirement	**At the Head office:** • Notebooks/Computers with the Windows operating system and Microsoft Office suite correctly licensed. • IP Phone system with a total of 3 devices. • Compatible with browsers: Chrome, Firefox, Edge, Safari. **At home:** • Notebooks/Computers with the Windows operating system and Microsoft Office suite correctly licensed. • Jabber software. • Internet connection. • Assign login rights to access the Active Directory system. • Log recording system for encrypting passwords through the VPN channel (AnyConnect). • Compatible with browsers: Chrome, Firefox, Edge, Safari.
Service Support	1. Through the Helpdesk center, which can be contacted through the following channels: 1.1 Call the HelpDesk at 02-821-7979. (The line is available 24x7) 1.2 Send an E-mail to helpdesk@mfec.co.th 1.3 Contact the designated person directly through the master provided in the E-mail 2. Through the application system: 2.1 Open https://mfec.service-now.com/ 2.2 Open https://ticketin.mfec.co.th 3. Receive service through E-mail Alert. * Annotation: Officer Helpdesk provide service 24x7

Service Target	*Service standards* Critical | Response Time: 15 minutes Resolution Time: 4 hours High | Response Time: 15 minutes Resolution Time: 8 hours Medium | Response Time: 15 minutes Resolution Time: 24 hours Low | Response Time: 15 minutes Resolution Time: 48 hours *Conditions except* When working with external clients, please consider the contracts that have been executed and ensure that all actions are in accordance with the specified terms and conditions of those contracts.
Operational Level Agreement	- IT Support team support BackOffice and TicketIn. - ITOMS.
Underpinning Contract	None
Delivery Scope	External customers across the country
Service Owner	Helpdesk
Service Status	Available

Service Name	CSOC
Standard Service Features	• Requesting backup and recovery for the main CSOC system, entry-exit system, and support systems at CSOC. • Requesting and granting access rights to spaces, networks, and VPNs, including various application systems. • Requesting CCTV camera recordings. • Installing, modifying, and canceling equipment related to log monitoring services. • Providing monitoring services with alerts, guidance, reporting, and participating in meetings as per the jointly agreed contract. • Monitoring news and notifying vulnerability issues in products. • Addressing and supporting customer-reported issues according to the jointly agreed contract. • Assisting with customer site incidents.
Service Hours	Tier 1 support 24x7 (Day Shift 07:00 AM - 08:00 PM, Night Shift 07:00 PM - 08:00 AM). Tier 2 support 8x5 (Monday - Friday 09:00 AM - 06:00 PM). Tier 3 on demand.
Service Support	1. Receive incidents through the E-mail address: csoc@mfec.co.th 2. Receive cases via phone number: 089-813-2015 3. Receive cases via Helpdesk
Service Requirement	**Customer-side log storage system** • Log storage system and the process of installing the log storage system. • Channels for log delivery and encryption of data transmission over the network. • Customers can prepare their own log storage system and delivery channels. **The system for receive and analyze logs** • Log storage space. • Log analysis system (SIEM). • Automation System (FortiSOAR) **Computer for analysis** • Desktop computers/laptops with licensed Windows. operating systems and Microsoft Office. • Supports Browsers: Chrome, Firefox, Edge, Safari. • VPN for accessing the MFEC network.

Service Support	• Receive incidents through the E-mail address: csoc@mfec.co.th • Receive cases via phone number: 089-813-2015 • Receive through CSOC services for external clients
Service Target	**Service standards** Critical/High: Response Time: 30 minutes Medium : Response Time: 24 hours Low: Response Time: 48 hours Response time starts from the event monitoring system, notifies from the monitoring screen 24x7 and the company responds to customers via telephone or E-mail (Response time only covered in parts time to detect and time to notify not including time to resolve). *conditions except* Consider contracts executed with external clients. To act i accordance with the contract.
Operational Level Agreement	• Network service (PROEN data center) • Service VPN (IT Support) • Service TicketIn (Helpdesk)
Underpinning Contract	• Purchasing a log analytics license system per year (FortiSIEM) • Purchase annual license for the automation management system (FortiSOAR) • Data Center Space and Internet Rental at CSOC Center • Building space rental SJ Infinite I Business Complex
Delivery Scope	Customers in Bangkok and its vicinity
Service Owner	CSOC
Service Status	Available

Service Name	InfoSec
Standard Service Features	-Product installation/update/decommission and dismantle -Post-sales support, Technical Support, Customer Support, Service Requests Handling, Troubleshooting and Defect Resolution. -Scheduled Maintenance are planned and conducted at regular intervals. (Preventive Maintenance).
Service Hours	SERVICE HOURS INCLUDE -24X7. -8X5 CUSTOMER STANDARD WORKING HOURS.
Service Requirement	1. The installation team verifies details from the Sales system, which specifies the Statement of Work (SOW). The team forwards this information to the InfoSec team. 2. Identify the responsible team by checking which team is accountable for the product. Assign the task to the responsible person, considering the nature of the assigned work. 3. Verification and Information Transfer: The installation team verifies details from the Sales system, particularly the Statement of Work (SOW), and forwards this information to the InfoSec team. 4. The team responsible for the product specifies the service provider, support, and issue resolution. This information is obtained by reviewing contracts with vendors.
Service Support	1. Through the Helpdesk center, which can be contacted through the following channels: 1.1 Call the HelpDesk at 02-821-7979 (The line is available 24x7) 1.2 Send an E-mail to helpdesk@mfec.co.th 1.3 Direct contact through the template specified in the E-mail. *Annotation: InfoSec Support Team is staff available 24x7*

Service Target	*Service standards* *Bangkok* • Installation, project-by-project based on deadline conditions, and tracking delays every 7 days based on workflows that there is a 10% delay from the target. by viewing the reports from the MPM system by sending e-mails to notify the relevant parties and there is a Dashboard page to confirm the results of delays the person in charge of the PM will follow up the cause of the delay of the problem. • Troubleshooting service ("For more information about the service level agreement (SLA) for our troubleshooting service, please refer to document MFEC-SMR-SD-002.") • Critical 15 mins, Onsite 4 hours (Response Time) • A minor NBD (non-business day) should be considered in accordance with the contract that has been executed with the service recipient. • Maintenance service is carried out according to contracts, depending on the device or product standards (Refer to the standard documentation on each device or product). *Vicinity* • Installation (SLA not specified) check from project Monthly meeting minutes and client meetings. • Troubleshooting service (There is a reference SLA document MFEC-SMR-SD-002) • Critical 15 mins, Onsite 8 hours (Response Time) • A minor NBD (non-business day) should be considered in accordance with the contract that has been executed with the service recipient. • Maintenance service is carried out according to contracts, depending on the device or product standards (Refer to the standard documentation on each device or product). *Provincial* • Installation (SLA not specified) V check from project Monthly meeting minutes and client meetings. • Troubleshooting service • Critical 15 mins, Onsite NBD (Response Time) Input a condition for identifying a case that will allow NBD to be processed. • A minor NBD (non-business day) should be considered in accordance with the contract that has been executed with the service recipient. • Maintenance service is carried out according to contracts, depending on the device or product standards (Refer to the standard documentation on each device or product).

Operational Level Agreement	• Helpdesk system supports 24x7 service. • MFEC internal products and customer site operations. • MPM program system that supports project and contract management.
Underpinning Contract	• Under the terms and conditions of the Call Center, Contact Center, and Hotline services provided in the product. • Agreement on the provision of backup equipment for MFEC customers.
Delivery Scope	Nationwide
Service Owner	InfoSec
Service Status	Available

Service Name	*System Infrastructure*
Standard Service Features	• Product installation/update/decommission and dismantle. • Post-sales support, Technical Support, Customer Support, Service Requests Handling, Troubleshooting and Defect Resolution. • Scheduled Maintenance are planned and conducted at regular intervals. (Preventive Maintenance).
Service Hours	Include: • 24x7 • 8x5 Customer standard working hours
Service Requirement	1. The installation team verifies details from the Sales system, which specifies the Statement of Work (SOW) and forwards it to the Engineering team. 2. Identify the team responsible for each product and assign tasks to the person responsible based on the nature of the job. 3. Products under responsibility are specified with the service provider, and support and issue resolution are considered by reviewing contracts with vendors.
Service Support	1. To contact the HelpDesk, you may use one of the following methods: 1.1 Call the HelpDesk at 02-821-7979 (The line is available 24x7) 1.2 Send an E-mail to helpdesk@mfec.co.th 1.3 Contact the designated person directly through the master provided in the e-mail *Annotation : Our Engineer's IT Support Team is available 24x7*

Service Target

Service standards

Bangkok

- Critical 15 mins, Onsite 4 hours (Response Time)
- A minor NBD (non-business day) should be considered in accordance with the contract that has been executed with the service recipient.
- Maintenance service based on contracts, depending on the device or product standards (Refer to the standards outlined documentation on each device or product).

Perimeter

- Installation (SLA not specified) View by project Monthly meeting minutes available and meeting with clients about customers
- Troubleshooting service (with SLA reference MFEC-SMR-SD-002)
- Critical 15 mins, Onsite 8 hours (Response Time)
- A minor NBD (non-business day) should be considered in accordance with the contract that has been executed with the service recipient.
- Maintenance operations are carried out in accordance with customer contracts and are tailored to each device's specific product standards. For more information on product standards for individual devices, please refer to the standard documentation provided for each device.

Provincial

- Recording assessments can help individuals maintain accurate records of meetings and discussions with clients. By keeping minutes of meetings and other important information, individuals can better track progress and ensure that all relevant details are properly documented.
- Our outage remediation services are defined based on the level of impact and access to the site. For more detailed information on these services, please refer to the documentation with the reference MFEC-SMR-SD-002.
- Critical 15 mins, Onsite NBD (Response Time) When identifying cases that will be processed as NBD, please include any relevant conditions that may impact the prioritization or handling of the case.
- A Minor NBD (non-business day) should be considered in accordance with the contract that has been executed with the service recipient.
- Maintenance operations are carried out in accordance with customer contracts and are tailored to each device's specific product standards. For more information on product standards for individual devices, please refer to the standard documentation provided for each device.

Operational Level Agreement	• System Helpdesk service support 24x7 • The MPM program system that supports project and contract management
Underpinning Contract	• On the conditions of the Call Center, Contact Center, Hotline of service providers in the product.
Delivery Scope	Customers outside the company nationwide
Service Owner	System Infrastructure
Service Status	Available

Service Name	*IT Support*
Standard Service Features	Our internal service offerings include: • Installation and maintenance of equipment/computers in the computer center. • User creation, authorization, password resets, revoking permissions, and access rights adjustments in Active Directory, E-mail, MPM, ESS, Proflex, i-solution, SharePoint, and Office 365. • Backup and restore systems and databases. • Monitoring and controlling access through Multi-Factor Authentication systems. • Cable installation and network device connections. • Software installation on the network. • Installation of malicious code prevention systems. • Configuration adjustments and updates for firewalls. • Internal support and problem resolution at the 2nd Line Support level within the organization. **Service Request/Incident Report Handling:** • Recording and tracking service requests until case closure. **External Service Provision:** • Preliminary problem resolution through remote communication systems with company clients.

Service Hours	• BackOffice • 8x5 Personnel Service for Problem Resolution
Service Requirement	1. Determine whether the equipment being supported is owned by MFEC or is listed in the maintenance register. 2. The site being managed must be within the terms of the service contract.
Service Support	1.Through the MFEC NOC (Network Operations Center), there are several contact channels available: 1.1 Telephone: 02-821-7811 (Operating hours: 8x5, excluding holidays) 1.2 E-mail Address: mfec_noc@mfec.co.th 1.3 Direct contact through the provided template in the e-mail.
Service Target	*The service standard* • View the document of MFEC-SMR-SD-002, the agreement for service provision.
Operational Level Agreement	• Service Network • Service InfoSec • Service System Infrastructure • Service CSOC • Service Helpdesk • Service Network • Service ISE • Service ITOMS
Underpinning Contract	• KIRZ Company: Supports both computer centers and external network systems. • True Company: Provides backup network support. • Microsoft Company: Supports the e-mail system. • Amazon Company: Provides DNS system support. • Cisco Company: Offers services such as MultiFactor Authentication, Mail Gateway, VPN, and Antivirus. • Ditto Company: Supports printer services. • ABIT Company: Provides air conditioning system maintenance. • Accurate Solution Company: Supports UPS maintenance. • Integrated Secure Company: Supports fire suppression system maintenance. • SiS Distribution (Thailand) Company: Supports network server maintenance.
Delivery Scope	Nationwide
Service Owner	IT Support
Service Status	Available

Service Name	ITOMS
Standard Service Features	• Provides services by personnel with expertise in information technology to customers under contracts, service level agreements (SLA), and other agreements made with the company. • Offers installation and maintenance services for information systems to customers.
Service Hours	Comprises: • Service delivery as per the contract.
Service Requirement	1.Contract information, Service Level Agreement (SLA), and other agreements made between the company and the customer. 2.The installation team reviews the details of the Sales system, which specifies the Scope of Work (SOW), to determine the work details. Subsequently, the information is forwarded to the Engineering team. 3.Evaluate the products or services to determine which team is responsible. Assign the task to the designated team member based on the nature of the responsibilities. 4.The responsible team for the product is identified, and the service provider, support, and issue resolution are specified by reviewing the contract with the vendor.
Service Support	1. Personnel will perform duties at the customer's site according to the specified duration in the contract. 2.Through the Helpdesk Service, which can be contacted through the following channels: 2.1 Phone number: 02-821-7979 (24x7 on business days) 2.2 E-mail Address: helpdesk@mfec.co.th
Service Target	Service Standard 1. Manage Service continuously in accordance with the contract. • Able to provide services to customers according to the contract, Service Level Agreement (SLA), and other agreements made by the company with customers. Details can be found in MFEC-SMR-SD-002. 2.Quality of on-site personnel • Evaluate the quality of service beyond the standards specified in the document MFEC-SMR-SD-002.
Operational Level Agreement	• The Helpdesk system supports 24x7 service. • The MPM software system supports project management and contract maintenance.

Underpinning Contract	Under the service conditions through various channels provided by each product's service provider, such as Call Center, Contact Center, Hotline, Web Portal, E-mail, etc.
Delivery Scope	Nationwide
Service Owner	ITOMS
Service Status	Available
ชื่อบริการ (Service Name)	*Network*
Standard Service Features	1. Installation/Upgrade/Removal of Cisco products and Aruba products 2. Post-sales support, addressing service requests, and resolving issues on Cisco products and Aruba products 3. Maintenance and servicing of Cisco products according to schedule (Preventive Maintenance) and Aruba products
Service Hours	Consists of • Gold Service 24x7 • Silver Service 8x5 or 9x5 • As specified in the contract under certain conditions
Service Requirement	1. Contract information, Service Level Agreement (SLA), and other agreements made with customers. 2. Installation team reviews details from the Sales system, specifying the Scope of Work (SOW), and forwards it to the Engineering team. 3. Evaluate products or services to determine which team is responsible and assign the task to the person in charge, considering the nature of the work. 4. The responsible team for the product specifies the service provider and supports problem resolution based on the agreement with the vendor.
Service Support	1. Personnel perform duties at the customer's site according to the specified contract duration. 2. On-site staff operate according to the customer's working hours or as specified in the contract. 3. Access support through the Helpdesk, which offers the following contact channels: 3.1 Phone: 02-821-7979 (The line is avaliable 24x7) 3.2 E-mail: helpdesk@mfec.co.th *Note: Engineers provide services 24x7.*

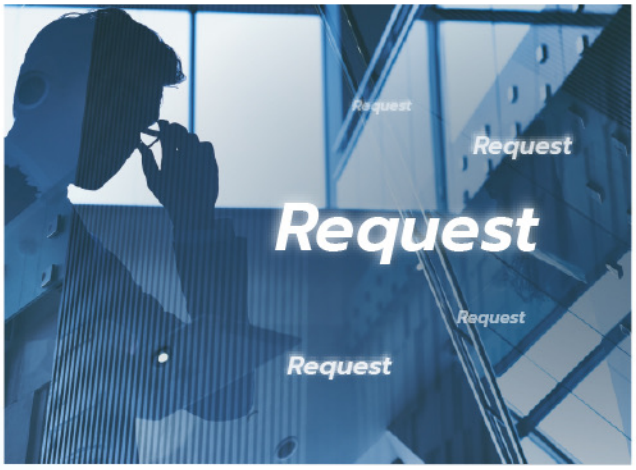
Service Target	*Service standards* Critical | Response Time: 10 minutes Resolution Time: 72 hours with no pending issues High | Response Time: 15 minutes Resolution Time: 72 hours, pending approval from the customer Medium | Response Time: 30 minutes Resolution Time: 72 hours Low | Response Time: 30 minutes Resolution Time: 72 hours *Exceptional Conditions:* Evaluate contracts with external customers to ensure compliance with the specified agreements.
Operational Level Agreement	• The Helpdesk system supports 24x7 service. • The MPM software system is designed to support project management and contracts.
Underpinning Contract	• Under the terms and conditions of the Call Center, Contact Center, Hotline of service providers in the product.
Delivery Scope	Nationwide
Service Owner	Network
Service Status	Available

Service Name	ISE
Standard Service Features	1.Post-sales support, addressing service requests, and resolving issues on products /Solution 2.Maintenance and servicing of products according to schedule (Preventive Maintenance)/Solution
Service Hours	Consists of • Gold Service 24x7 • Silver Service 8x5 or 9x5 As specified in the contract under certain conditions
Service Requirement	• Contract information, Service Level Agreement (SLA), and other agreements made with customers. • Installation team reviews details from the Sales system, specifying the Scope of Work (SOW), and forwards it to the Engineering team. • Evaluate products or services to determine which team is responsible and assign the task to the person in charge, considering the nature of the work. • The responsible team for the product specifies the service provider and supports problem resolution based on the agreement with the vendor.
Service Support	1. officer will perform work at the client's site according to the duration specified in the service contract. 2. officer on-site will operate according to the client's working hours or as specified in the contract 3. To contact the HelpDesk, you may use one of the following methods: 3.1 Call the HelpDesk at 02-821-7979 (The line is available 24x7 on workdays) 3.2 Contact the designated person directly through the master provided in the e-mail : helpdesk@mfec.co.th Annotation: Engineer officer provided service support 24x7
Service Target	*Bangkok Service standards* Critical | Response Time: 15 minutes Resolution Time: 4 hours, with no pending issues High | Response Time: 15 minutes Resolution Time: 8 hours, pending approval from the customer Medium | Response Time: 15 minutes Resolution Time: 24 hours, pending approval from the customer Low | Response Time: 15 minutes Resolution Time: 72 hours, pending approval from the customer Maintenance service based on contracts, depending on the device or product standards (Refer to the standards outlined documentation on each device or product).

เป้าหมายการให้บริการ (Service Target)	*Perimeter* Critical | Response Time: 15 minutes Resolution Time: 6 hours, with no pending issues High | Response Time: 15 minutes Resolution Time: 8 hours, pending approval from the customer Medium | Response Time: 15 minutes Resolution Time: 24 hours, pending approval from the customer Low | Response Time: 15 minutes Resolution Time: 72 hours, pending approval from the customer Maintenance service based on contracts, depending on the device or product standards (Refer to the standards outlined documentation on each device or product). *Peripheral provinces* Service for Resolving Issues • Critical 15 minutes, Onsite NBD (Response Time) add conditions for specifying the acceptance of cases that will lead to NBD processing • Minor NBD • Maintenance service based on contracts, depending on the device or product standards (Refer to the standards outlined documentation on each device or product). *Exemption Conditions* For contracts executed with external clients, ensure that they are conducted in accordance with the specified contract terms.
Operational Level Agreement	• Helpdesk service support 24x7 • The MPM program system that supports project and contract management
Underpinning Contract	Under the terms and conditions of the Call Center, Contact Center, Hotline of service providers in the product.
Delivery Scope	Nationwide
Service Owner	ISE
Service Status	Available

Incident Management

Our outage management process involves taking action to resolve service disruptions after they have been reported to our HelpDesk (1st Line Support). Our team works quickly to restore services and minimize any impact on our customers' business operations.



Service Request Management

Service requests from customers that do not involve incidents (i.e. Incident Requests) will be handled according to the terms of the service agreement, as if they were incidents.

5

Effectiveness of the SMS

Service Level Agreement (SLA):
Service agreements SLA provide a standard for requiring services to customers according to the agreement.

Definition of SLA in each topic

- ***Severity*** *Refers to the level of impact that requires urgent correction.*
- ***Response Time*** *Refers to the time taken to respond to the correction requests from relevant agencies.*
- ***Restoration Time*** *Refers to the period needed to restore normal operations after a disruption or outage.*

Severity	*Impact level* Consider 4 levels by type of customer	*Level of urgency* Consider 4 levels
CRITICAL	Impact on customers and corporate image	The business was damaged at that time.
HIGH	Impact within the organization	Damaged business but can be executed
MEDIUM	Impact at the department level within the organization	Damaged business at an acceptable level
LOW	Personal impact	The business was not affected or had very little impact.

SLA of each service Details are as follows:

1. Helpdesk

Severity	Response Time	Restoration Time*	Responsible
CRITICAL	15 MINUTES	4 HOURS	Helpdesk ↓ 2nd Line Support ↓ Supplier / Vendor
HIGH	15 MINUTES	8 HOURS	
MEDIUM	15 MINUTES	24 HOURS	
LOW	15 MINUTES	48 HOURS	

*Conditions will be considered in conjunction with the customer according to the contract.

2. Cyber Security Operation Center and Manage Security (CSOC)

Severity*	Response Time**	Responsible
CRITICAL	30 MINUTES	CSOC 1st Tier → CSOC 2nd Tier → IT Support
HIGH		
MEDIUM	24 HOURS	
LOW	48 HOURS	CSOC 1st Tier → CSOC 2nd Tier → IT Support The information is summarized as a daily report. If an attemptis made to access the system/network

Note:

* Conditions are referenced with the specified threshold values of monitoring devices, and consideration i given in conjunction with direct customer notifications.

** The conditions for incidents adhere primarily to the terms of the contract implemented in collaboration with the customer.

3. Information Security (InfoSec)

Severity	Response Time	Onsite*	Resolution Time	Responsible
CRITICAL	15 MINUTES	**BANGKOK** Implemented within 4 hours	Processed within 72 hours with no pending conditions.	Helpdesk ↓ 2nd Line Support ↓ Supplier/Vendor
HIGH	15 MINUTES	**PERIMETER :** Implemented within 8 hours		
MEDIUM	15 MINUTES	**PROVINCIAL :** processed within the next day	Process within 72 hours.	
LOW	15 MINUTES	**BANGKOK AND PERIMETER :** carry on inside 8 hours **PROVINCIAL :** processed within the next day		

*Note: * Conditions will be considered in conjunction with the customer according to the contract.*

4. System Infrastructure

Severity	Response Time	Onsite*	Resolution Time	Responsible
CRITICAL	15 MINUTES	**BANGKOK** Implemented within 4 hours	Processed within 72 hours with pending conditions.	Helpdesk ↓ 2nd Line Support ↓ Supplier/Vendor
HIGH	15 MINUTES	**PERIMETER :** Implemented within 8 hours	Processed within 72 hours, pending actions require coordination with the customer.	
MEDIUM	15 MINUTES	**PROVINCES :** processed within the next day	Processed within 72 hours.	
LOW	15 MINUTES	**BANGKOK AND PERIMETER :** Implemented within 8 hours **PROVINCES :** processed within the next day		

*Note: * Conditions will be considered in conjunction with the customer according to the contract.*

5. IT Support

Severity	Response Time	Restoration Time	Condition
SEV-1 (CRITICAL)	30 MINUTES	within 1 working days	The system provides core services in the scope of implementation in the ISO/IEC 27001 standard and equipment to support the main work system unable to respond to users
SEV-2 (HIGH)	1 HOUR	within 3 working days	Core services outside the scope of implementation in ISO/IEC 27001 are unable to respond to users.
SEV-3 (MEDIUM)	4 HOURS	within 5 working days	Support work system that does not affect the main work system and the work system used within the organization It affects only departments that do not affect customers directly.
SEV-4 (LOW)	8 HOURS	within 10 working days	Back-up systems, systems used within the organization no business impact

***Note**: The current incident escalation process supports the escalation of incidents by 1 level, from 1st Line Support to 2nd Line Support. If there is no action at the 2nd Level, the system administrator will prepare a report for management.*

6. IT Operation Manage Service (ITOMS)

Severity	Response Time	Onsite*	Resolution Time	Responsible
CRITICAL	15 MINUTES	**Gold Service 24x7** **Peripheral provinces:** Within 6 hours **other provinces:** Within NBD **Silver Service 9x5** **Peripheral provinces:** Within 6 hours **other provinces:** Within NBD (Within business hours from 9:00 AM to 6:00 PM) Bangkok: Coordination with Engineers and Vendors.	Resolve the issue within 1 hour with conditions.	Helpdesk ↓ Engineer ↓ 2nd Tier Engineer
HIGH	15 MINUTES		Resolve the issue within 12 hours.	
MEDIUM	15 MINUTES		Resolve the issue within 48 hours.	
LOW	15 MINUTES	Coordinate with Engineers and Vendors in Bangkok	Resolve the issue within 7 days.	

***Note**: Conditions will be considered in conjunction with the customer according to the contract.*

7. Networking and Cisco Customer Experience (Network)

Severity	Response Time	Onsite*	Resolution Time	Responsible
CRITICAL	10 MINUTES	**Gold Service 24x7** **Bangkok**: Within 4 hours **Peripheral provinces**: Within 6 hours **Other provinces**: Next Day (NBD) **Silver Service 9x5** **Bangkok**: Within 4 hours **Peripheral provinces**: Within 6 hours **Other provinces**: Next Day (NBD)	Operational response within 72 hours.	Helpdesk ↓ L1-Cisco ↓ L2-Cisco
HIGH	15 MINUTES		Operational response within 72 hours. Pending activities should be coordinated with customers only.	
MEDIUM	30 MINUTES		Operational response within 72 hours.	
LOW	30 MINUTES	Service Request Support		Helpdesk ↓ L1-Cisco

8. Infrastructure Services Excellence (ISE)

Severity	Response Time	Onsite*	Resolution Time	Responsible
CRITICAL	10 MINUTES	**GOLD SERVICE 24X7** BANGKOK: WITHIN 4 HOURS PERIPHERAL PROVINCES: WITHIN 6 HOURS OTHER PROVINCES: NEXT DAY (NBD) **SILVER SERVICE 9X5** BANGKOK: WITHIN 4 HOURS PERIPHERAL PROVINCES: WITHIN 6 HOURS OTHER PROVINCES: NEXT DAY (NBD)	OPERATIONAL RESPONSE WITHIN 72 HOURS.	Helpdesk ↓ ISE Engineer ↓ L2-Product
HIGH	15 MINUTES		OPERATIONAL RESPONSE WITHIN 72 HOURS. PENDING ACTIVITIES SHOULD BE COORDINATED WITH CUSTOMERS ONLY.	
MEDIUM	15 MINUTES			
LOW	15 MINUTES	BANGKOK AND PERIMETER : PROCESSED WITHIN 8 HOURS PERIPHERAL PROVINCES : PROCESSED WITHIN THE NEXT BUSINESS DAY (NBD)	OPERATIONAL RESPONSE WITHIN 72 HOURS.	Helpdesk ↓ ISE Engineer ↓ L2-Product

If there is an inconsistency in the provision of services, the operators should consider implementing improvements accordingly based on the SMS requirements. These inconsistenciesmay arise from various sources such as reviewer's review results (auditor), customer feedback, and risk assessment.

Internal case reporting channel

MFEC_NOC@mfec.co.th

External case reporting channel

helpdesk@mfec.co.th

02-821-7979

Examples of Internal Service Request

- User creation on AD for Outsource
- Reinstallation of OS on client machines
- Delegation of user access to the supervisor or assigned person when the user has left the job
- Password reset on AD in case of forgetting password
- Request for permission to use systems such as NAV, PF, I-Solution, SharePoint Permission
- Creation of group mail
- Access problems related to VPN Duo or different systems
- Resource allocation on Vmware as per requirement
- IP assignment for new devices or servers
- Back up and restore of Database
- Edit, add, or delete policies and pools in Web Application Firewall (WAF)
- Change, edit or delete DNS in Domain Name Server (DNS)
- Request to allow Firewall
- Change, edit or delete DNS in External DNS
- Change, edit or delete policy, SMTP routing in Mail Gateway IMSVA.

Examples of External issue

- Server/Systems/Node/Device Down.
- Application Down.
- Port/Link down.
- Link flaps.
- System/Storage/ Network Hardware Fail.
- Firewall issue.
- Network Connection Fail.
- Can't Start Service
- Can't access or use application.
- Services Unavailable.
- Software Failure/Software bug
- Error Messages, Logs, Debugs.
- CPU/Memury High usage
- Upgrade software Fail.
- Job fail / Backup fail.

Can study the details Services Management Policy More information is available SharePoint of the company ISO_20000