IT Support Documents

1. IT Support Policies and Procedures

IT Service Desk Policy

- **Purpose: Outlines the role and responsibilities of the IT Service Desk in handling employee requests and incidents.**
- **Components:**
  - **Service Desk Availability: Hours of operation (e.g., 9 AM - 6 PM, Monday to Friday), including emergency after-hours contact.**
  - **Communication Channels: Available channels for reporting issues (e.g., phone, email, self-service portal, chat).**
  - **Response Time SLAs:**
    - **High Priority: Critical issues (e.g., system outages) - Response within 15 minutes, resolution within 2 hours.**
    - **Medium Priority: Non-critical but important issues (e.g., software malfunction) - Response within 1 hour, resolution within 8 hours.**
    - **Low Priority: Minor issues (e.g., minor UI bugs) - Response within 4 hours, resolution within 48 hours.**
  - **Escalation Procedure: Steps for escalating unresolved issues to higher support levels.**
  - **Employee Responsibilities: Guidelines on reporting issues, including information to provide (e.g., screenshots, error codes).**

IT Asset Management Policy

- **Purpose: Defines procedures for managing and maintaining IT assets, including hardware, software, and licenses.**
- **Components:**
  - **Asset Inventory: Maintenance of a centralized inventory of all IT assets, including laptops, desktops, servers, mobile devices, software licenses, and peripherals.**
  - **Asset Allocation: Guidelines for issuing assets to employees, including approval processes and documentation.**

    - **Asset Tracking: Procedures for tracking asset location, condition, and assignment to employees.**
    - **Asset Disposal: Safe and compliant disposal of end-of-life IT assets, including data wiping and recycling.**
    - **Software Licensing: Compliance with software licensing agreements, including monitoring and renewing licenses.**

Data Privacy and Security Policy

- **Purpose: Ensures the protection of organizational data from unauthorized access and breaches.**
- **Components:**
    - **Data Access Controls: Use of role-based access control (RBAC) to restrict access to sensitive data.**
    - **Data Encryption: Encryption requirements for data in transit and at rest, including email communication.**
    - **Password Management: Guidelines for creating and managing secure passwords, including multi-factor authentication (MFA).**
    - **Incident Response: Steps to be taken in case of a data breach, including reporting, containment, and communication.**
    - **Employee Training: Regular training on data privacy practices, phishing prevention, and recognizing social engineering.**

Remote Work IT Policy

- **Purpose: Provides guidelines and best practices for employees working remotely to ensure productivity and security.**
- **Components:**
    - **Approved Tools and Software: List of company-approved communication, collaboration, and project management tools.**
    - **Network Security: Use of Virtual Private Networks (VPNs) for accessing company resources securely.**
    - **Device Security: Requirements for using company-issued or personal devices (e.g., antivirus, firewalls).**
    - **Data Backup: Regular backups of work-related data, including use of cloud services.**

    - **Remote Support: Process for obtaining IT support remotely, including remote desktop assistance tools.**

---

2. IT Support Process Documents

Incident Management Process

- **Purpose: To define a standardized approach for managing IT incidents to restore normal service as quickly as possible.**
- **Steps:**
    1. **Incident Identification: User reports an issue through the designated channels.**
    2. **Logging: Service desk logs the incident with a unique ID, captures all relevant details (e.g., user details, time of incident, symptoms).**
    3. **Classification and Prioritization: Incident is classified (hardware, software, network) and prioritized (high, medium, low).**
    4. **Investigation and Diagnosis: IT support team investigates the issue, identifies the root cause, and determines the appropriate resolution.**
    5. **Resolution and Recovery: Fix is applied, and service is restored. Confirmation from the user that the issue is resolved.**
    6. **Closure: Incident is formally closed in the IT service management system with notes on resolution steps.**
    7. **Post-Incident Review: Review of the incident to identify improvements in processes or systems.**

Change Management Process

- **Purpose: Ensure that all changes to IT services and infrastructure are systematically planned, tested, and implemented to minimize disruption.**
- **Steps:**
    1. **Request for Change (RFC): Formal request submitted by the stakeholder or IT team to propose a change.**
    2. **Impact Analysis: Evaluation of the potential impact on the system, network, and users.**
    3. **Approval Process: Change Advisory Board (CAB) reviews and approves or rejects the proposed change.**

4. Testing: Change is tested in a controlled environment to assess the potential impact and risks.
5. Implementation: Approved change is implemented during a planned maintenance window.
6. Verification: Post-implementation verification to ensure the change works as expected.
7. Documentation: Update of all relevant documentation, including configuration management database (CMDB).

IT Maintenance Process

- Purpose: Regular and proactive maintenance of IT systems and equipment to prevent failures and ensure optimal performance.
- Tasks:
  - Routine Check-Ups: Regular inspection of servers, network devices, and critical software.
  - Patch Management: Application of security patches and updates to operating systems, applications, and hardware firmware.
  - System Backup: Scheduled backups of critical data and configuration files.
  - Performance Monitoring: Continuous monitoring of system performance, including server loads, network traffic, and application performance.

---

3. IT Support Forms and Templates

IT Support Request Form

- Fields:
  - Employee Information: Name, Employee ID, Department, Contact Information.
  - Issue Details: Brief description of the problem, date/time of occurrence, screenshots (if applicable).
  - Priority Level: High, Medium, Low.
  - Preferred Contact Method: Phone, Email, Chat.

Access Request Form

- Fields:
    - Employee Information: Name, Employee ID, Department.
    - Access Type Requested: Type of access (e.g., new user creation, password reset, additional permissions).
    - Reason for Access: Justification for access.
    - Manager Approval: Signature of the employee's manager authorizing the request.

Incident Report Form

- Fields:
    - Incident ID: Unique identifier for the incident.
    - Reported By: Employee details.
    - Incident Description: Full description of the incident, including symptoms, frequency, and impact.
    - Steps Taken: Initial steps taken by the user or support to mitigate the issue.
    - Resolution Steps: Actions taken by the IT team to resolve the incident.
    - Resolution Confirmation: Confirmation by the employee that the issue is resolved.
    - Follow-Up: Notes for any follow-up actions required.

---

4. IT Security Documents

IT Security Policy

- Purpose: Establishes guidelines for protecting organizational data, systems, and networks against unauthorized access, breaches, and attacks.
- Components:
    - Acceptable Use Policy: Guidelines on appropriate use of company IT resources (e.g., internet usage, downloading software).
    - Password Policy: Rules for creating strong passwords, mandatory password changes, and storage of credentials.
    - Antivirus and Anti-Malware: Requirements for installing and updating antivirus software on all devices.

    - Email Security: Protocols for handling phishing, spam, and suspicious attachments.
    - Access Control: Measures to control access to sensitive data, including role-based access and least privilege principle.
    - Incident Reporting: Steps for employees to report any suspicious activity or security incidents.
    - Regular Audits: Schedule for regular security audits and vulnerability assessments.

Business Continuity and Disaster Recovery Plan

- Purpose: To ensure that critical business functions can continue during and after a disaster or disruptive event.
- Components:
    - Business Impact Analysis: Identification of critical business functions and the impact of their disruption.
    - Recovery Strategies: Plans for data recovery, system restoration, and alternative operations (e.g., use of cloud services).
    - Communication Plan: Steps for communicating with stakeholders, employees, and customers during a disaster.
    - Testing and Maintenance: Regular testing of the disaster recovery plan and updating based on test results or changes in the environment.

---

5. IT Knowledge Base Articles

Common Troubleshooting Guides

- Topics:
    - Network Connectivity Issues: Steps to troubleshoot network connectivity problems (e.g., checking router settings, resetting the network adapter).
    - Printer Setup and Troubleshooting: Guide to setting up printers and troubleshooting common printer errors (e.g., paper jams, driver issues).
    - Software Installation: Instructions for installing and configuring common business software (e.g., Microsoft Office, Adobe Acrobat).

  - **Email Issues: Troubleshooting email problems, such as login issues, sending/receiving errors, and managing mailbox size.**

User Guides

- **Topics:**
  - **VPN Access Guide: Step-by-step instructions for connecting to the company VPN, including troubleshooting common issues.**
  - **Remote Access Guide: Guidelines for accessing company resources remotely, including use of remote desktop tools.**
  - **Cybersecurity Awareness Guide: Tips and best practices for recognizing phishing attempts, managing passwords, and protecting personal and company data.**

IT Support Policies and Procedures

Incident Response Policy

- **Purpose**: Provides guidelines for responding to IT incidents and emergencies to minimize impact and recover swiftly.
- **Components**:
  - **Incident Response Team (IRT)**: Composition and roles of the team responsible for incident response.
  - **Incident Categorization**: Classification of incidents (e.g., security breach, system failure) and associated response procedures.
  - **Communication Protocols**: Guidelines for internal and external communication during and after an incident.
  - **Post-Incident Analysis**: Process for reviewing incidents to identify lessons learned and improvements.

Service Continuity Policy

- **Purpose**: Ensures IT services can continue during and after disruptive events.
- **Components**:
  - **Continuity Planning**: Strategies for maintaining critical services during disruptions.
  - **Business Impact Analysis (BIA)**: Assessment of critical business functions and their dependencies.

    - **Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)**: Definitions of acceptable downtime and data loss limits.
    - **Testing and Exercises**: Regular testing of continuity plans and exercises to prepare staff.

IT Support Process Documents

Request Fulfillment Process

- **Purpose**: Standardizes the process for handling service requests from users.
- **Steps**:
    - **Request Submission**: Methods for users to submit requests (e.g., online portal, email).
    - **Request Logging**: Capturing details of the request, including user information and request type.
    - **Request Categorization**: Classification of requests (e.g., new software, hardware upgrades).
    - **Fulfillment**: Execution of the request, including installation, configuration, or provisioning.
    - **Request Closure**: Verification of request fulfillment and closing of the request ticket.

Problem Management Process

- **Purpose**: Manages and resolves underlying problems that cause incidents.
- **Steps**:
    - **Problem Detection**: Identification of problems from patterns in incidents.
    - **Problem Analysis**: Investigation to determine root causes and contributing factors.
    - **Workarounds**: Implementation of temporary fixes to mitigate impact while permanent solutions are developed.
    - **Solution Implementation**: Permanent resolution of the problem and prevention of recurrence.
    - **Knowledge Base Updates**: Documenting solutions and workarounds in the knowledge base.

IT Support Forms and Templates

Service Catalog

- **Purpose**: Provides a comprehensive list of IT services available to users.
- **Fields**:
    - **Service Description**: Detailed explanation of each IT service.
    - **Service Categories**: Grouping of services by type (e.g., hardware support, software installation).
    - **Request Process**: Steps to request each service, including forms and approval requirements.
    - **Service Levels**: SLAs associated with each service, including response and resolution times.

User Access Review Form

- **Fields**:
    - **User Information**: Name, Employee ID, Department.
    - **Current Access Rights**: List of current access permissions.
    - **Review Findings**: Evaluation of current access rights and any discrepancies.
    - **Action Required**: Recommended changes to access permissions.

IT Security Documents

Security Incident Management Policy

- **Purpose**: Establishes procedures for managing and resolving security incidents.
- **Components**:
    - **Incident Reporting**: Methods for reporting security incidents.
    - **Incident Classification**: Categories of security incidents (e.g., malware, unauthorized access).
    - **Incident Handling**: Procedures for investigating and responding to incidents.
    - **Incident Recovery**: Steps for restoring systems and data after an incident.

Vulnerability Management Policy

- **Purpose**: Manages vulnerabilities in IT systems to protect against threats.

- **Components**:
    - **Vulnerability Assessment**: Regular scanning and assessment of vulnerabilities.
    - **Risk Assessment**: Evaluation of the potential impact and likelihood of identified vulnerabilities.
    - **Remediation**: Actions to address and fix vulnerabilities.
    - **Reporting**: Documentation and reporting of vulnerabilities and remediation efforts.

IT Knowledge Base Articles

System Configuration Guides

- **Topics**:
    - **Server Configuration**: Detailed instructions for configuring servers, including hardware and software settings.
    - **Network Configuration**: Guidelines for configuring network devices (e.g., routers, switches) and services.
    - **Application Configuration**: Steps for configuring business applications, including custom settings and integrations.

User Training Materials

- **Topics**:
    - **Basic IT Skills**: Training materials for basic IT skills, including using common software and hardware.
    - **Advanced Features**: Guides for advanced features and functionalities of IT systems and applications.
    - **Troubleshooting Guides**: Self-help guides for users to troubleshoot common IT issues.