

Fictitious Company Employee IT Handbook

Table of Contents

1. **Introduction**
2. **IT Support Services**
 - Incident Reporting
 - Service Requests
 - Change Requests
 - Problem Management
 - Access Requests
 - Hardware Requests
 - Software Support
 - Network Support
 - Printer and Peripheral Support
 - Mobile Device Support
 - User Account Management
3. **IT Policies**
 - Acceptable Use Policy
 - Data Protection Policy
 - Password Policy
 - Remote Work Policy
 - Software Installation Policy
 - BYOD (Bring Your Own Device) Policy
 - Email and Communication Policy
 - Backup and Recovery Policy
 - Internet Usage Policy
 - System Monitoring Policy
4. **IT Resources**
 - Contact Information
 - IT Portal Access
 - Training and Documentation
 - Frequently Asked Questions (FAQs)
 - IT Service Catalog
5. **Security Guidelines**
 - Phishing Awareness
 - Secure Browsing
 - Device Security
 - Social Engineering Awareness
 - Physical Security
 - Data Encryption
 - Malware Protection
 - Firewall Configuration
6. **Compliance and Audit**
 - Internal Audits
 - External Audits
 - Reporting Violations
 - Regulatory Compliance
 - Audit Trail Policy

7. Appendices

- ITSM Template Numbers
 - Glossary of Terms
 - IT Service Level Agreements (SLAs)
-

1. Introduction

Welcome to Fictitious Company! This IT Handbook is designed to provide you with essential information about IT services and policies. Please review this document thoroughly to ensure effective and secure utilization of our IT resources.

2. IT Support Services

Incident Reporting

Template Number: INC001

Procedure:

1. Identify the issue.
2. Log the incident via the IT Portal using template INC001.
3. Provide detailed information including:
 - Description of the issue
 - Impact on business
 - Urgency level

Service Requests

Template Number: SRV001

Procedure:

1. Determine the type of service required.
2. Log the request via the IT Portal using template SRV001.
3. Provide detailed information including:
 - Type of service requested
 - Reason for the request
 - Expected outcome

Change Requests

Template Number: CHG001

Procedure:

1. Identify the change needed.
2. Log the change request via the IT Portal using template CHG001.
3. Provide detailed information including:
 - Description of the change
 - Reason for the change
 - Impact assessment
 - Approval from relevant stakeholders

Problem Management

Template Number: PRB001

Procedure:

1. Identify the underlying problem.
2. Log the problem via the IT Portal using template PRB001.
3. Provide detailed information including:
 - Description of the problem
 - Related incidents
 - Proposed solution

Access Requests

Template Number: ACC001

Procedure:

1. Identify the access needed.
2. Log the access request via the IT Portal using template ACC001.
3. Provide detailed information including:
 - User information
 - Systems or data required
 - Reason for access

Hardware Requests

Template Number: HW001

Procedure:

1. Identify the hardware needed.
2. Log the hardware request via the IT Portal using template HW001.
3. Provide detailed information including:
 - Type of hardware requested
 - Reason for the request
 - Expected usage

Software Support

Template Number: SW001

Procedure:

1. Identify the software issue or request.
2. Log the software support request via the IT Portal using template SW001.
3. Provide detailed information including:
 - Description of the issue or request
 - Software name and version
 - Impact on business

Network Support

Template Number: NET001

Procedure:

1. Identify the network issue or request.
2. Log the network support request via the IT Portal using template NET001.

3. Provide detailed information including:
 - Description of the issue or request
 - Affected device(s)
 - Error messages received

Printer and Peripheral Support

Template Number: PRT001

Procedure:

1. Identify the printer or peripheral issue or request.
2. Log the support request via the IT Portal using template PRT001.
3. Provide detailed information including:
 - Description of the issue or request
 - Device model and serial number
 - Connection type (USB, network, etc.)

Mobile Device Support

Template Number: MDB001

Procedure:

1. Identify the mobile device issue or request.
2. Log the support request via the IT Portal using template MDB001.
3. Provide detailed information including:
 - Description of the issue or request
 - Device model and operating system
 - Error messages received

User Account Management

Template Number: UAM001

Procedure:

1. Identify the account management request (creation, modification, deletion).
2. Log the request via the IT Portal using template UAM001.
3. Provide detailed information including:
 - User information
 - Type of request
 - Reason for the request

3. IT Policies

Acceptable Use Policy

All employees must use company IT resources responsibly and in accordance with company policies.

Data Protection Policy

Employees are required to protect sensitive company data.

Password Policy

- Passwords must be at least 8 characters long.
- Include a mix of uppercase, lowercase, numbers, and special characters.
- Change passwords every 90 days.

Remote Work Policy

Guidelines for employees working remotely:

- Use a VPN to access company resources.
- Keep all company data on secure, company-approved devices.

Software Installation Policy

No unauthorized software installations.

BYOD Policy

Guidelines for using personal devices for work:

- Install company-approved security software.
- Keep the device updated with the latest security patches.

Email and Communication Policy

Use company email for business communications.

Backup and Recovery Policy

Guidelines for data backup and recovery.

Internet Usage Policy

Appropriate use of the internet on company networks.

System Monitoring Policy

Company's right to monitor IT systems.

4. IT Resources

Contact Information

- IT Helpdesk: helpdesk@fictitiouscompany.com
- IT Department: it@fictitiouscompany.com
- Phone Support: 1-800-555-1234

IT Portal Access

[IT Portal](#)

Training and Documentation

Available on the IT Portal.

Frequently Asked Questions (FAQs)

Quick answers to common IT questions.

IT Service Catalog

List of available IT services.

5. Security Guidelines

Phishing Awareness

Be cautious of suspicious emails or messages.

Secure Browsing

Use approved browsers and avoid unsecured websites.

Device Security

Keep devices updated and use antivirus software.

Social Engineering Awareness

Be wary of tactics used to gain sensitive information.

Physical Security

Secure documents and devices.

Data Encryption

Encrypt sensitive data.

Malware Protection

Use and update anti-malware tools.

Firewall Configuration

Follow company guidelines for firewall settings.

6. Compliance and Audit

Internal Audits

Regular audits to ensure compliance.

External Audits

Third-party audits for industry standards.

Reporting Violations

Report policy violations to the IT Helpdesk.

Regulatory Compliance

Adherence to industry regulations (e.g., GDPR, HIPAA).

Audit Trail Policy

Maintain records for audit purposes.

7. Appendices

ITSM Template Numbers

Service Type	Template Number
Incident Reporting	INC001
Service Requests	SRV001
Change Requests	CHG001
Problem Management	PRB001
Access Requests	ACC001
Hardware Requests	HW001
Software Support	SW001
Network Support	NET001
Printer and Peripheral Support	PRT001

Service Type	Template Number
--------------	-----------------

Mobile Device Support	MDB001
-----------------------	--------

User Account Management	UAM001
-------------------------	--------

Glossary of Terms

- **ITSM:** Information Technology Service Management
- **VPN:** Virtual Private Network
- **BYOD:** Bring Your Own Device

IT Service Level Agreements (SLAs)

Details available on the IT Portal.

Thank you for reading the Fictitious Company Employee IT Handbook. For further assistance, please contact the IT Helpdesk.