IT Security Guidelines

Document Type: Microsoft Word (.docx)

Created: 2025-06-07

Purpose: Test document for RAG system ingestion

# Introduction

This document outlines the essential IT security guidelines that all employees must follow   
 to protect our organization's digital assets and maintain compliance with industry standards.

# Password Security

Strong passwords are the first line of defense against cyber threats.

## Password Requirements:

• Minimum 12 characters in length  
• Include uppercase and lowercase letters  
• Include at least one number  
• Include at least one special character  
• Avoid dictionary words or personal information  
• Change passwords every 90 days

# Multi-Factor Authentication (MFA)

MFA is required for all business applications and systems. This adds an extra layer of   
 security by requiring a second form of verification beyond your password.

## Supported MFA Methods:

• Authenticator apps (Google Authenticator, Microsoft Authenticator)  
• SMS text messages  
• Hardware security keys  
• Biometric authentication (fingerprint, face recognition)

# Email Security

Email is a common vector for cyber attacks. Follow these guidelines to protect yourself   
 and the organization from email-based threats.

## Best Practices:

• Verify sender identity before clicking links or downloading attachments  
• Be suspicious of urgent requests for sensitive information  
• Report phishing attempts to the security team  
• Use encrypted email for sensitive communications  
• Keep software and email clients updated

# Data Protection

Protecting sensitive data is everyone's responsibility. This includes customer information,   
 financial data, intellectual property, and personal employee information.

## Data Classification Levels:

|  |  |  |
| --- | --- | --- |
| Classification | Description | Examples |
| Public | Information that can be freely shared | Marketing materials, press releases |
| Internal | Information for internal use only | Employee directories, internal policies |
| Confidential | Sensitive business information | Financial reports, customer lists |
| Restricted | Highly sensitive information | Personal data, trade secrets |

# Security Incident Reporting

If you suspect a security incident, report it immediately to the security team.   
 Quick reporting can help minimize damage and prevent further compromise.

## What to Report:

• Suspected malware infections  
• Unauthorized access attempts  
• Lost or stolen devices  
• Suspicious emails or phone calls  
• Data breaches or unauthorized data access

# Emergency Contacts

Security Team: security@company.com or ext. 9999 (24/7)  
 IT Help Desk: helpdesk@company.com or ext. 4357  
 HR Department: hr@company.com or ext. 4200

==================================================

This document is confidential and proprietary. Distribution is restricted to authorized   
 personnel only. For questions or clarifications, contact the IT Security team.  
   
 Document Version: 1.3  
 Last Updated: 2025-06-07  
 Next Review Date: 2025-12-07