Document 1: IT Infrastructure Access Policy

Title: IT Infrastructure and System Access Policy

Department: Information Technology

Effective Date: January 15, 2024

Document ID: IT-POL-2024-001

1. System Access Guidelines

All employees requiring access to internal systems must follow these procedures:

New Employee Access:

Submit access request via ServiceNow portal (ticket category: "New User Setup")

Approval required from direct manager and department head

Standard access granted within 24 hours of approval

Special permissions (admin, database) require additional security clearance

VPN Access:

GlobalProtect VPN client must be installed

Two-factor authentication (2FA) mandatory

VPN credentials expire every 90 days

Troubleshooting: contact helpdesk@company.com or extension 4111

Password Policy:

Minimum 12 characters with upper, lower, numbers, special characters

Password rotation every 60 days

Do not share credentials under any circumstances

Password manager: LastPass (company license available)

2. Software Installation Procedure
Approved Software List:

Development: VS Code, IntelliJ IDEA, Docker Desktop, Postman

Collaboration: Slack, Microsoft Teams, Zoom

Productivity: Office 365 suite, Adobe Acrobat Pro

Installation Process:

Self-service via Software Center (Windows) or Managed Software Center (Mac)

For unavailable software, submit request with business justification

Security team reviews within 48 hours

Prohibited: Unlicensed software, torrent clients, unauthorized remote access tools

License Management:

Annual license audit conducted every November

Unused licenses reclaimed after 30 days of inactivity

Specialized software (CAD, Data Analytics) requires project code

3. API Documentation Access

Internal APIs:

Gateway URL: https://api.internal.company.com

Authentication: OAuth2 with client credentials

Rate limit: 1000 requests/minute per application

Documentation: Available at Confluence > Tech > API Documentation

Third-party API Integration:

Register application in API Developer Portal

Obtain client ID and secret from API team

Test environment: https://api-sandbox.company.com

Production access requires security review

Troubleshooting Common Issues:

401 Unauthorized: Check token expiration (tokens valid for 1 hour)

429 Too Many Requests: Implement exponential backoff

503 Service Unavailable: Check status dashboard at status.company.com

4. Network and Connectivity

Wi-Fi Access:

Secure network: "Company-Secure" (WPA2 Enterprise)

Guest network: "Company-Guest" (24-hour access, separate password)

IoT devices: Register MAC address with network team

Remote Development Setup:

Dev servers accessible via SSH on port 2222

Jump host: jumpbox.dev.company.com

Database access: Via bastion host only

File transfer: Use SFTP to sftp.company.com

5、Security Protocols

Incident Reporting:

Security incidents: security@company.com (immediate response)

Phishing emails: Forward to phishing@company.com

Lost devices: Report within 1 hour to helpdesk

Data Classification:

Public: Marketing materials, job postings

Internal: Meeting notes, project plans

Confidential: Source code, customer data, financials

Restricted: Passwords, encryption keys

Encryption Requirements:

Full disk encryption mandatory on all laptops

HTTPS required for all web applications

Database encryption at rest for PII data