4.1 Purpose

Protect Unisoftwares' digital assets, client data, and intellectual property from unauthorized access, cyber threats, and data breaches.

4.2 Device Management

4.2.1 Laptop/Desktop Issuance

- **Company-owned devices**: Dell, HP, Lenovo laptops (Windows or macOS for designers/developers)
- **Specifications**: Minimum i5/Ryzen 5, 8GB RAM, 256GB SSD
- **Ownership**: Device remains company property, must be returned on exit
- **Personal Use**: Limited personal use allowed (no illegal/inappropriate content)

4.2.2 Mobile Device Management (MDM)

- All company devices must be enrolled in MDM system
- Remote wipe capability enabled
- Security patches auto-installed
- Lost/stolen device = report immediately to IT

4.2.3 BYOD (Bring Your Own Device)

- Allowed with manager approval
- Must install company security apps
- Company data must be in separate work profile
- Company reserves right to wipe corporate data remotely

4.3 Password & Authentication Policy

4.3.1 Password Requirements

- **Minimum Length**: 12 characters
- **Complexity**: Mix of uppercase, lowercase, numbers, special characters
- **No Common Passwords**: No "password123", "company123", etc.
- **Password Manager Required**: Use LastPass, 1Password, or Bitwarden

4.3.2 Multi-Factor Authentication (MFA)

- **Mandatory** for all corporate accounts:
  - Email (Office 365)
  - Slack
  - AWS/Cloud platforms
  - Project management tools
  - CRM systems
- **MFA Methods**: Authenticator app (Google Authenticator, Authy), SMS backup

4.3.3 Password Sharing

- **Never share passwords** via email, Slack, or verbal communication
- Use password manager sharing features for team credentials
- Service accounts must use single sign-on (SSO) where possible

4.3.4 Password Reset

- Self-service password reset available via MFA
- IT support can reset after identity verification
- Emergency access: Contact IT help desk

4.4 Network & Remote Access

4.4.1 VPN (Virtual Private Network)

- **Mandatory** when accessing internal resources from outside office
- VPN software: Cisco AnyConnect or company-provided solution
- Always-on VPN for remote workers
- No split tunneling (all traffic through VPN)

4.4.2 Wi-Fi Security

- **Office Wi-Fi**: WPA3 encrypted, password protected
- **Guest Wi-Fi**: Separate network, no access to internal systems
- **Public Wi-Fi**: Use VPN when working from cafes, airports

4.4.3 Remote Desktop Access

- Use company-approved remote desktop tools only
- Screen sharing requires approval for sensitive data
- Recording client calls: Obtain consent first

4.5 Data Classification & Handling

4.5.1 Data Categories

Public

- Marketing materials, published blog posts
- No special handling required

Internal

- Company policies, internal memos, project plans
- Share only with employees
- Mark documents "Internal Use Only"

Confidential

- Client contracts, financial data, employee records
- Encrypted storage required
- Share on need-to-know basis
- Mark documents "Confidential"

Highly Confidential

- Source code, client passwords, payment data
- Encrypted + access logs
- Extremely restricted access
- Mark documents "Highly Confidential - Restricted"

4.5.2 Data Storage

- **Client Data**: Store in designated client folders (Google Drive/SharePoint)
- **Source Code**: GitHub/GitLab (private repositories)

- **Personal Data**: CRM system only (no local spreadsheets)
- **Backups**: Automated daily backups (encrypted)

4.5.3 Data Transmission

- **Email**: Use encrypted email for confidential data
- **File Sharing**: Use company-approved tools (Google Drive, Dropbox Business)
- **Large Files**: Use secure file transfer (WeTransfer Pro, Send)
- **Never use**: Personal email, personal Dropbox, WhatsApp for client data

---

4.6 Email & Phishing Security

4.6.1 Email Best Practices

- Check sender address carefully (beware of spoofing)
- Hover over links before clicking
- Don't open suspicious attachments
- Verify unusual requests (especially money transfers) via phone call

4.6.2 Phishing Red Flags

- Urgent requests for passwords or payment
- Spelling/grammar errors
- Unexpected attachments or links
- Sender email doesn't match domain

4.6.3 Reporting Suspicious Emails

- **Do NOT** click links or reply
- Forward to: security@unisoftwares.pk
- Delete email after reporting
- IT will investigate and alert team if necessary

4.7 Software & Application Security

4.7.1 Approved Software

- Only install software from company-approved list
- Request new software via IT ticket
- No pirated/cracked software (legal risk + malware)

4.7.2 Software Updates

- **Auto-updates enabled** for OS and critical software
- Patch Tuesday: Install security updates within 7 days
- Browser updates: Keep Chrome/Firefox/Edge up to date

4.7.3 Browser Extensions

- Minimize browser extensions (security risk)
- Approved extensions: LastPass, Grammarly, Loom
- No unauthorized ad blockers or VPN extensions

4.8 Incident Response

4.8.1 Security Incident Reporting

Report immediately to IT/Security team if you:

- Suspect malware infection
- Click on phishing link
- Lose company device
- Accidentally share confidential data
- Notice unauthorized access to accounts

Contact: security@unisoftwares.pk or call IT emergency line

4.8.2 Incident Response Process

1. **Contain**: Disconnect device from network
2. **Report**: Notify IT immediately (within 1 hour)
3. **Investigate**: IT/Security team investigates
4. **Remediate**: Clean/reimage device, reset passwords
5. **Document**: Incident logged, lessons learned

6. **Notify**: Inform affected parties if data breach

4.8.3 Data Breach Protocol

- **Assessment**: Determine scope and severity
- **Notification**: Inform affected clients within 72 hours (GDPR)
- **Remediation**: Fix vulnerability, enhance security
- **Legal Compliance**: Follow local data protection laws

4.9 Social Engineering Awareness

4.9.1 Common Tactics

- **Pretexting**: Attacker creates fake scenario to get info
- **Baiting**: Offering something (USB drive, download) to install malware
- **Tailgating**: Following employee into secure area
- **Quid Pro Quo**: Offering service in exchange for information

4.9.2 Defense Strategies

- Verify identity before sharing information
- Challenge unknown people in office
- Don't plug in unknown USB drives
- Be skeptical of "too good to be true" offers

4.10 Acceptable Use Policy

4.10.1 Permitted Uses

- Business communication and collaboration
- Research related to work projects
- Limited personal use (lunch break browsing)

4.10.2 Prohibited Uses

- Accessing illegal, adult, or gambling websites
- Downloading pirated content

- Cryptocurrency mining on company devices
- Harassment, cyberbullying, hate speech
- Unauthorized disclosure of company information
- Using company resources for personal business

4.10.3 Monitoring & Privacy

- Company reserves right to monitor device usage
- No expectation of privacy on company devices
- Monitoring for security and compliance only
- Personal communications should use personal devices

FAQs (IT Security)

Q1: Do I need MFA for all accounts?
A: Yes, MFA is mandatory for email, Slack, AWS, and all corporate systems. (Source: IT_Security_Policy.pdf, Section 4.3.2)

Q2: Can I use public Wi-Fi for work?
A: Only with VPN enabled. Never access sensitive data on public Wi-Fi without VPN. (Source: IT_Security_Policy.pdf, Section 4.4.2)

Q3: What should I do if I click a phishing link?
A: Immediately report to security@unisoftwares.pk, change passwords, and disconnect device. (Source: IT_Security_Policy.pdf, Section 4.8.1)

Q4: Can I install software on my work laptop?
A: Only company-approved software. Submit request via IT ticket. (Source: IT_Security_Policy.pdf, Section 4.7.1)