IT SECURITY POLICY
Version 2.1 - Effective January 2024

===================
PASSWORD REQUIREMENTS
===================

All employees must follow these password guidelines:

Minimum Requirements:
- At least 12 characters long
- Must include uppercase letters (A-Z)
- Must include lowercase letters (a-z)
- Must include numbers (0-9)
- Must include special characters (!@#$%^&*)
- Cannot contain your name or username
- Cannot reuse last 5 passwords

Password Changes:
- Passwords must be changed every 90 days
- System will send reminder 7 days before expiration
- Temporary lockout after 5 failed login attempts
- Contact IT helpdesk to unlock account

===================
DATACLASSIFICATION
===================

All company data is classified into three categories:

PUBLIC:
- Marketing materials
- Published reports
- Public website content
- No special handling required

INTERNAL:
- Business plans
- Financial reports
- Employee directories
- Requires login to access
- Cannot be shared externally without approval

CONFIDENTIAL:
- Customer data
- Trade secrets
- Legal documents
- Encryption required
- Access restricted to authorized personnel only
- Cannot be stored on personal devices

===================
DEVICE SECURITY
===================

Laptop and Desktop Requirements:
- Full disk encryption must be enabled
- Automatic screen lock after 5 minutes of inactivity
- Antivirus software must be installed and updated
- Operating system updates must be applied within 7 days
- VPN required when working remotely

Mobile Devices:
- Must be enrolled in Mobile Device Management (MDM)
- PIN or biometric lock required
- Remote wipe capability must be enabled
- Company email can only be accessed through approved apps

===================
REMOTE WORK POLICY
===================

Security Requirements for Remote Workers:

Network Security:
- Use company VPN for all work activities
- Never use public WiFi without VPN
- Home router must use WPA3 encryption
- Change default router password

Physical Security:
- Lock your computer when stepping away
- Ensure privacy when on video calls
- Do not discuss confidential matters in public spaces

- Secure all company devices when traveling

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

INCIDENT REPORTING
===================

Report security incidents immediately:

What to Report:

- Lost or stolen devices
- Suspicious emails or phishing attempts
- Unauthorized access to systems
- Data breaches or leaks
- Malware infections

How to Report:

1. Email: security@company.com
2. Phone: Extension 5555 (24/7 hotline)
3. Submit ticket through IT portal

Response Time:

- Critical incidents: Immediate response
- High priority: Within 1 hour
- Medium priority: Within 4 hours
- Low priority: Within 24 hours

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

ACCEPTABLE USE
===================

Company Resources:

- Company devices are for business use primarily
- Limited personal use is acceptable during breaks
- No illegal downloads or streaming
- No visiting inappropriate websites
- No sharing login credentials

Email Guidelines:

- Use professional language
- Do not send confidential data via email without encryption
- Be cautious of phishing emails
- Report suspicious emails to IT security

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

CONSEQUENCES

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

Policy Violations:

- First offense: Written warning
- Second offense: Suspension
- Third offense: Termination

Serious violations (data breach, intentional security compromise):

- Immediate termination
- Possible legal action
- Law enforcement notification if required

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

TRAINING

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

All employees must complete:

- Security awareness training annually
- Phishing simulation tests quarterly
- Role-specific security training as assigned

New employees must complete security training within first week of employment.