IT SECURITY POLICY

Version 2.1 - Effective January 2024

==========

PASSWORD REQUIREMENTS

==========

All employees must follow these password guidelines to maintain system security:

MINIMUM REQUIREMENTS:

Your password must meet ALL of these criteria:

- At least 12 characters long (longer is better)
- 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, username, or company name
- Cannot contain common words or patterns (password123, qwerty, etc.)
- Cannot reuse any of your last 5 passwords

GOOD PASSWORD EXAMPLES:

- MyC0mpany!2024$Secure
- Tr@vel#Plan2024&Go
- B1ue$Sky*Morning!23

BAD PASSWORD EXAMPLES:

- Password123! (too common)

- JohnSmith2024 (contains name)

- 12345678!Aa (predictable pattern)

PASSWORD CHANGES:

- Passwords must be changed every 90 days

- System will send email reminder 7 days before expiration

- You'll see a warning banner 3 days before expiration

- On expiration day, you'll be forced to change password at next login

ACCOUNT LOCKOUT:

- Temporary lockout after 5 failed login attempts

- Lockout duration: 30 minutes

- After 3 lockouts in 24 hours, account is disabled

- Contact IT helpdesk at ext. 5555 to unlock account immediately

HOW TO CHANGE YOUR PASSWORD:

1. Log into the employee portal at portal.company.com

2. Click your profile icon in the top right

3. Select "Security Settings"

4. Click "Change Password"

5. Enter your current password

6. Enter your new password (must meet all requirements)

7. Confirm your new password

8. Click "Update Password"

9. You'll receive a confirmation email

FORGOTTEN PASSWORD:

If you forget your password:

1. Go to the login page

2. Click "Forgot Password" link

3. Enter your employee email address

4. Check your email for a reset link (arrives within 5 minutes)

5. Click the link (valid for 1 hour only)

6. Create a new password

7. Log in with your new password

If you don't receive the reset email within 10 minutes, contact IT helpdesk.

PASSWORD MANAGER:

The company recommends using a password manager (1Password, LastPass, or Bitwarden) to:

- Generate strong, unique passwords

- Store passwords securely

- Auto-fill login forms

- Sync passwords across devices

Contact IT for approved password manager options and setup assistance.

==========

DATA CLASSIFICATION

==========

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 to minimize damage and protect company assets.

WHAT TO REPORT:

You must report these incidents immediately:

Critical (Report within 15 minutes):

- Lost or stolen devices containing company data
- Confirmed data breach or leak
- Ransomware or malware infection
- Unauthorized access to confidential systems
- Physical security breach

High Priority (Report within 1 hour):

- Suspicious emails or phishing attempts
- Unusual account activity

- Compromised passwords or credentials
- Unauthorized software installation
- Security policy violations by others

Medium Priority (Report within 4 hours):
- Potential security vulnerabilities
- Suspicious network activity
- Lost access badges or keys
- Concerns about data handling

HOW TO REPORT:

Use these methods to report security incidents (use multiple if critical):

Method 1: Email
- Address: security@company.com
- Include: Your name, date/time, detailed description, affected systems
- Attach: Screenshots or evidence if available
- Response time: Within 1 hour for critical issues

Method 2: Phone
- Number: Extension 5555 (internal) or 1-800-SEC-HELP (external)
- Available: 24/7 hotline
- Best for: Urgent or critical incidents
- Response time: Immediate for critical issues

Method 3: IT Portal

- URL: portal.company.com/security

- Click: "Report Security Incident"

- Fill out: Incident report form with all details

- Best for: Non-urgent incidents or detailed reporting

WHAT INFORMATION TO PROVIDE:

When reporting an incident, include:

1. Your name and contact information

2. Date and time the incident occurred

3. Date and time you discovered it

4. Detailed description of what happened

5. Systems or data affected

6. Actions you've already taken

7. Any evidence (screenshots, emails, logs)

8. Potential impact or damage

RESPONSE TIMES:

The security team will respond based on severity:

Critical incidents:

- Initial response: Immediate (within 15 minutes)

- Security team dispatched: Within 30 minutes

- Incident contained: Within 2 hours

- Full investigation: Within 24 hours

High priority:

- Initial response: Within 1 hour
- Investigation started: Within 4 hours
- Resolution: Within 24 hours

Medium priority:
- Initial response: Within 4 hours
- Investigation: Within 2 business days
- Resolution: Within 5 business days

Low priority:
- Initial response: Within 24 hours
- Investigation: Within 5 business days
- Resolution: Within 10 business days

AFTER REPORTING:

Once you report an incident:

1. You'll receive an incident ticket number via email
2. Security team will contact you for additional information
3. Follow any instructions provided by the security team
4. Do not attempt to fix the issue yourself unless instructed
5. Preserve all evidence (don't delete emails, logs, etc.)
6. Document everything you remember about the incident
7. Cooperate fully with the investigation

CONFIDENTIALITY:

All security incidents are treated confidentially. Information is shared only with:

- Security team members

- Your direct manager (if necessary)

- Legal team (for serious incidents)

- Law enforcement (if required by law)

You will not face retaliation for reporting security incidents in good faith, even if you accidentally caused the incident.

==========

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 mandatory security training:

ANNUAL REQUIREMENTS:

- Security awareness training (2 hours, online)

- Phishing simulation tests (quarterly, 15 minutes each)

- Role-specific security training as assigned by your manager

- Data protection and privacy training (1 hour)

NEW EMPLOYEE TRAINING:

New employees must complete security training within the first week of employment as part of the onboarding process. This includes:

Day 1-2: Security Basics (3 hours total)

- Password policy and best practices
- Device security requirements
- Acceptable use policy
- Physical security procedures

Day 3-5: Advanced Security (2 hours total)

- Data classification and handling
- Incident reporting procedures
- Remote work security
- Email and phishing awareness

The training is delivered through our learning management system at training.company.com. Your manager will enroll you automatically during onboarding. You must pass the final assessment with 80% or higher.

TRAINING SCHEDULE:

- New employees: First week (mandatory)
- Annual refresher: Every January (mandatory)
- Phishing tests: Quarterly (mandatory)
- Role-specific: As assigned (varies by role)

FAILURE TO COMPLETE:

- First reminder: 3 days before deadline

- Second reminder: 1 day before deadline

- Overdue: Account access restricted until training is complete

- Repeated failures: Disciplinary action

TRAINING CONTACT:

For questions about security training:

- Email: training@company.com

- Phone: Extension 5556

- Portal: training.company.com/support