ProtectUsKids

Cybersecurity & Information Security Policy

Effective Date: January 1, 2026
Draft Updated: December 31, 2025

1. PURPOSE AND SCOPE

This Cybersecurity & Information Security Policy establishes security standards for protecting Protect Us Kids Foundation's ("PUK") information assets, systems, and data.

PURPOSE:

- Protect confidential and sensitive information, especially data related to children
- Ensure availability, integrity, and confidentiality of systems and data
- Comply with legal and regulatory requirements
- Prevent unauthorized access, use, disclosure, or destruction of information
- Establish clear security responsibilities
- Minimize security risks and incidents

SCOPE:

This policy applies to:

- All PUK employees, interns, volunteers, contractors, and board members
- All information systems, networks, devices, and data
- All organizational and personal devices used for PUK business
- All third-party vendors and partners with access to PUK systems or data

2. INFORMATION CLASSIFICATION

PUK classifies information into categories requiring different levels of protection:

RESTRICTED (Highest Security)

- Children's personally identifiable information
- Safeguarding incident reports

- Financial account credentials
- Legal documents and attorney-client communications
- Donor financial information
- Personnel records and background checks

CONFIDENTIAL (High Security)

- Internal operational documents
- Donor contact information
- Strategic plans and proposals
- Vendor contracts
- Employee information (non-sensitive)
- Program participant data (non-identifying)

INTERNAL USE (Moderate Security)

- Internal communications
- Meeting notes and agendas
- Draft documents
- General operational information

PUBLIC (General Security)

- Website content
- Published reports and materials
- Press releases
- Educational resources

3. ACCESS CONTROL

PRINCIPLE OF LEAST PRIVILEGE:

- Users receive minimum access necessary for their role
- Access rights reviewed quarterly
- Temporary access provided for specific projects with defined end dates
- Access immediately revoked upon separation

USER AUTHENTICATION:

- Strong passwords required: minimum 12 characters, mix of uppercase, lowercase, numbers, symbols
- Password changes every 90 days for high-security accounts
- No password reuse (last 5 passwords)

- Multi-factor authentication (MFA) required for:
- Email accounts
- Financial systems
- Systems containing children's data
- Administrative access
- Remote access

ACCOUNT MANAGEMENT:

- Unique user accounts (no shared accounts)
- Default passwords changed immediately
- Accounts locked after 5 failed login attempts
- Inactive accounts disabled after 90 days
- Guest/temporary accounts approved by supervisor, limited duration

4. DEVICE SECURITY

ORGANIZATIONAL DEVICES:

- Full disk encryption required
- Automatic screen lock after 10 minutes of inactivity
- Anti-virus/anti-malware software installed and updated
- Operating systems and software kept current with security patches
- Firewall enabled
- Automatic backups configured

PERSONAL DEVICES (BYOD):

If personal devices are used for PUK work:

- Must meet minimum security requirements
- Separate accounts/profiles for work data preferred
- PUK reserves right to remotely wipe organizational data
- Device passcode/biometric lock required
- Lost or stolen devices reported immediately

MOBILE DEVICE SECURITY:

- Passcode or biometric authentication required
- Automatic lock after 5 minutes
- Encryption enabled
- Remote wipe capability enabled
- Restricted data must not be stored on mobile devices without approval

REMOVABLE MEDIA:

- USB drives and external storage must be encrypted
- Scanning for malware before use
- Restricted data on removable media requires approval
- Secure disposal when no longer needed

5. NETWORK SECURITY

WIRELESS NETWORKS:

- WPA3 or WPA2 encryption required
- Strong passwords (minimum 16 characters)
- Guest networks isolated from organizational network
- Default router passwords changed
- Firmware kept updated

REMOTE ACCESS:

- Virtual Private Network (VPN) required for remote access to systems
- MFA required for VPN access
- Remote desktop connections secured and monitored
- No split-tunneling (all traffic through VPN)

PUBLIC WI-FI:

- Use VPN when accessing organizational systems on public Wi-Fi
- Avoid accessing restricted data on public networks
- Disable file sharing and automatic connectivity
- Verify network authenticity before connecting

6. DATA PROTECTION

ENCRYPTION:

- Data at rest: Encryption required for restricted and confidential data
- Data in transit: TLS 1.2 or higher for all web communications
- Email: Encrypted email required for restricted data
- Backups: Encrypted before storage

DATA HANDLING:

- Restricted data handled only by authorized personnel

- Minimum necessary principle: collect and retain only what is needed
- Secure disposal when no longer needed (see Data Retention Policy)
- No storage on personal cloud services (Dropbox, iCloud, etc.) without approval

BACKUPS:

- Critical systems backed up daily
- Backups encrypted and stored securely
- Backup restoration tested quarterly
- Off-site backup maintained

DATA TRANSFERS:

- Secure file transfer protocols (SFTP, HTTPS)
- Encrypted email attachments for restricted data
- Secure file sharing services approved by IT
- Physical media encrypted and tracked

7. EMAIL AND COMMUNICATION SECURITY

EMAIL SECURITY:

- Do not click suspicious links or open unexpected attachments
- Verify sender identity before responding to sensitive requests
- Use encrypted email for restricted data
- Do not send passwords via email
- Report phishing attempts to IT
- Use caution with email forwarding

PHISHING AWARENESS:

Be alert for phishing indicators:

- Urgent requests for action or credentials
- Requests to verify account information
- Suspicious sender addresses or domains
- Poor grammar or unusual formatting
- Unexpected attachments or links

INSTANT MESSAGING:

- Use approved business communication platforms
- Do not share restricted data via instant messaging

- Verify recipient identity for sensitive discussions
- Enable encryption when available

8. INTERNET AND WEB SECURITY

WEB BROWSING:

- Keep browsers updated
- Do not disable security features
- Be cautious of downloads from untrusted sources
- Verify website authenticity (HTTPS, valid certificates)
- Clear cache and cookies on shared/public computers

SOCIAL MEDIA:

- Use separate accounts for personal and organizational purposes
- Do not share confidential information on social media
- Verify requests before connecting with unknown individuals
- Enable privacy settings
- Be mindful of information that could be used for social engineering

9. PHYSICAL SECURITY

WORKPLACE SECURITY:

- Lock screens when leaving workstations
- Do not leave devices unattended in public
- Secure documents containing restricted data in locked areas
- Visitors escorted in office areas
- Shred confidential documents before disposal

DEVICE SECURITY:

- Cable locks for laptops in offices
- Report lost or stolen devices immediately
- Do not leave devices in visible areas of vehicles
- Secure devices during travel

10. THIRD-PARTY AND VENDOR SECURITY

VENDOR MANAGEMENT:

- Security assessment before engagement
- Data Processing Agreements (DPAs) required
- Vendors must meet minimum security standards
- Annual security reviews for critical vendors
- Access removed promptly when relationship ends

CLOUD SERVICES:

- Approved cloud services only
- Evaluate security practices before adoption
- Configure security settings appropriately
- Regular review of access permissions
- Encryption for stored data

11. INCIDENT RESPONSE

SECURITY INCIDENTS:

Report immediately if you:

- Suspect a security breach or data exposure
- Lose a device containing organizational data
- Fall victim to phishing or social engineering
- Notice unusual system behavior or unauthorized access
- Receive suspicious communications

REPORTING PROCEDURE:

- Notify supervisor and IT immediately
- Do not attempt to investigate or remediate on your own
- Preserve evidence (do not delete files, clear logs, etc.)
- Document what occurred and when

INCIDENT RESPONSE:

- Contain the incident to prevent further damage
- Investigate root cause and scope
- Remediate vulnerabilities
- Notify affected individuals as legally required
- Document incident and response
- Conduct post-incident review

12. CHILD DATA PROTECTION - SPECIAL REQUIREMENTS

Enhanced security measures for children's data:

- Segregated storage with additional encryption
- Strictly limited access (need-to-know only)
- Enhanced monitoring and audit trails
- No storage on mobile devices without explicit approval
- Annual security audits of systems containing children's data
- Immediate incident response for any suspected compromise

Child Sexual Abuse Material (CSAM):

- Never download, save, or forward suspected CSAM
- Report immediately to NCMEC CyberTipline
- Do not open suspected files
- Preserve original URLs or metadata for reporting
- Contact supervisor for support

13. SECURITY AWARENESS AND TRAINING

REQUIRED TRAINING:

- New employee/volunteer orientation: Security basics
- Annual refresher training: All personnel
- Specialized training: Roles handling restricted data
- Phishing awareness: Quarterly simulations

TRAINING TOPICS:

- Password security and MFA
- Phishing and social engineering
- Data classification and handling
- Device security
- Incident reporting
- Child data protection requirements
- Regulatory compliance (COPPA, GDPR, etc.)

14. COMPLIANCE AND MONITORING

SECURITY ASSESSMENTS:

- Annual vulnerability scans

- Periodic penetration testing
- Quarterly access reviews
- Annual policy review

MONITORING:

- Log collection and review
- Intrusion detection
- Unusual activity alerts
- Security event correlation

AUDITS:

- Internal audits: Annual
- External audits: As required by funders or regulations
- Review findings and implement corrections

15. ROLES AND RESPONSIBILITIES

EXECUTIVE DIRECTOR:

- Overall accountability for information security
- Approve security policies
- Allocate resources for security

ALL PERSONNEL:

- Follow security policies and procedures
- Protect credentials and access
- Report security incidents
- Complete required training

IT STAFF / VENDORS:

- Implement technical security controls
- Monitor systems for threats
- Respond to security incidents
- Maintain security documentation

SUPERVISORS:

- Ensure team members complete training
- Approve access requests

- Report and respond to incidents
- Model good security practices

16. CONSEQUENCES OF NON-COMPLIANCE

Violations of this policy may result in:

- Retraining
- Restricted access privileges
- Written warning
- Suspension
- Termination of employment or volunteer status
- Legal action (if criminal activity involved)

Severity of consequences depends on:

- Nature and severity of violation
- Intent (negligence vs. malicious)
- Impact on organization or individuals
- Previous violations

17. RELATED POLICIES

This policy should be read with:

- Privacy Policy
- Acceptable Use Policy
- Data Retention Policy
- Safeguarding & Child Protection Policy
- Bring Your Own Device (BYOD) Policy (if separate)
- Remote Work Policy

18. POLICY REVIEW

This policy will be reviewed:

- Annually at minimum
- After significant security incidents
- When technology or threats change
- When regulatory requirements change

Updates approved by: Executive Director and Board of Directors

19. CONTACT INFORMATION

For security questions or to report incidents:

IT Support: [IT contact email/phone]
Privacy Officer: privacy@protect-us-kids.org

General: info@protect-us-kids.org | 866.772.3354

For emergencies involving child safety:
NCMEC CyberTipline: https://report.cybertip.org | 1-800-843-5678