<Place Your Org Name Here>

CYBER SECURITY POLICY

[Company Name]
Cybersecurity Policy
Version: 1.0
Effective Date: [Insert Date]
Approved By: Board of Directors / Executive Director

---

1. PURPOSE

The purpose of this Cybersecurity Policy is to establish the framework by which [Organization Name] protects its information systems, sensitive data, donors, clients, staff, and stakeholders from cybersecurity threats.

As a nonprofit organization, we recognize our responsibility to safeguard:

- Personally Identifiable Information (PII)
- Protected Health Information (PHI) (if applicable)
- Payment Card Information (PCI)
- Donor records
- Financial data
- Confidential program data
- Grant and federal reporting information

This policy supports compliance with applicable regulations including (as applicable):

- HIPAA / HITECH
- PCI-DSS
- GDPR
- State data privacy laws
- Federal grant cybersecurity requirements
- FCC program security obligations

---

2. SCOPE

This policy applies to:

- All employees
- Volunteers
- Board members
- Contractors
- Consultants
- Third-party service providers
- Any individual with access to organizational systems or data

This policy applies to all systems owned, leased, managed, or used by the organization, including:

- On-premise servers
- Cloud platforms (Microsoft 365, Google Workspace, etc.)
- Email systems
- Laptops, desktops, tablets
- Mobile devices
- Network infrastructure
- VoIP systems
- SaaS applications

---

3. GOVERNANCE & OVERSIGHT

The Executive Director (or designated IT Lead) is responsible for cybersecurity oversight.

The Board of Directors shall:

- Receive annual cybersecurity updates
- Review risk assessments
- Approve major cybersecurity investments
- Ensure compliance with regulatory requirements

---

4. RISK MANAGEMENT

The organization shall:

- ☐ Conduct an annual cybersecurity risk assessment
- ☐ Maintain a risk register
- ☐ Identify critical systems and data
- ☐ Evaluate vendor security practices
- ☐ Document mitigation plans

Risk assessments shall include evaluation of:

- Phishing exposure
- Ransomware risk
- Data breach exposure
- Cloud misconfiguration
- Insider threats
- Business continuity risk

---

5. ACCESS CONTROL

5.1 Least Privilege

Access to systems and data shall be granted based on:

- Job role
- Operational necessity
- Minimum required permissions

5.2 Account Management

- ☐ Unique user accounts required
- ☐ Shared accounts prohibited (except approved service accounts)
- ☐ Terminated employees removed within 24 hours
- ☐ Quarterly access reviews conducted

---

6. PASSWORD & AUTHENTICATION POLICY

- ☐ Minimum 12-character passwords required
- ☐ Password manager recommended
- ☐ Password reuse prohibited across systems
- ☐ Multi-Factor Authentication (MFA) required for:
  - Email
  - Cloud platforms
  - Financial systems
  - Administrator accounts
  - Remote access

---

7. ENDPOINT & DEVICE SECURITY

- ☐ All devices must have antivirus/endpoint protection
- ☐ Devices must be encrypted
- ☐ Automatic updates enabled
- ☐ Firewall enabled
- ☐ Screen lock after inactivity
- ☐ Lost/stolen devices reported immediately

Remote work devices must meet the same standards as office devices.

---

8. NETWORK SECURITY

- ☐ Business-grade firewall deployed
- ☐ Default passwords removed from networking equipment
- ☐ Guest Wi-Fi separated from internal network
- ☐ Regular firmware updates applied
- ☐ VPN required for remote administrative access

---

9. DATA PROTECTION & CLASSIFICATION

Data shall be classified as:

- Public
- Internal
- Confidential
- Restricted

Restricted data includes:

- PHI
- Donor payment information
- SSNs
- Bank account data
- Background checks

Security controls shall align with classification level.

---

10. DATA BACKUP & RECOVERY

- ☐ Daily automated backups performed
- ☐ Backups encrypted
- ☐ At least one backup stored offsite or in cloud
- ☐ Quarterly restore testing performed
- ☐ Disaster recovery plan documented

---

11. EMAIL & PHISHING PROTECTION

- ☐ Email filtering enabled
- ☐ DMARC, SPF, DKIM configured
- ☐ Phishing awareness training conducted annually
- ☐ Suspicious emails reported to IT immediately

---

12. INCIDENT RESPONSE

The organization shall maintain a documented Incident Response Plan that includes:

- Incident identification
- Containment procedures
- Notification protocols
- Legal/regulatory reporting
- Communication plan
- Post-incident review

All suspected breaches must be reported immediately to:
[Insert Reporting Contact]

---

13. VENDOR & THIRD-PARTY RISK MANAGEMENT

- ☐ Vendors must sign data protection agreements
- ☐ Business Associate Agreements (BAA) required if handling PHI
- ☐ Vendor cybersecurity reviewed before onboarding
- ☐ Annual vendor security reassessment conducted

---

14. REGULATORY COMPLIANCE

If applicable, the organization shall maintain compliance with:

HIPAA (If Handling PHI)

- ☐ Risk assessment completed
- ☐ BAA agreements executed
- ☐ Access controls enforced

PCI-DSS (If Processing Credit Cards)

- ☐ Secure payment processor used
- ☐ Cardholder data not stored locally
- ☐ Quarterly vulnerability scans (if required)

GDPR (If Serving EU Residents)

- ☐ Data subject rights process established
- ☐ Data minimization practices followed

---

15. SECURITY AWARENESS & TRAINING

- ☐ Annual cybersecurity training required
- ☐ New employee onboarding includes security training
- ☐ Board receives cybersecurity briefing annually
- ☐ Periodic phishing simulations conducted

---

16. AI & EMERGING TECHNOLOGY SECURITY

If AI tools are used:

- ☐ AI access restricted to approved users
- ☐ No PHI entered into public AI systems without safeguards
- ☐ Data governance policies enforced
- ☐ AI usage policy adopted

---

17. ENFORCEMENT

Failure to comply with this policy may result in:

- Access revocation
- Disciplinary action
- Termination
- Legal consequences

---

18. POLICY REVIEW

This policy shall be reviewed:

- ☐ Annually
- ☐ After major security incidents
- ☐ After regulatory changes

ACKNOWLEDGMENT

I acknowledge that I have read and understand this Cybersecurity Policy and agree to comply with its provisions.

Name: _____

Signature: _____

Date: _____
