Cedric Dean Holdings, Inc.

Peer Support NC Program
Cyber Attack Response & Information Security Policy

---

1. Policy Title

Cyber Attack Response, Prevention, and Information Security Policy

---

2. Effective Date

Effective: January 21, 2026
Review Cycle: Annual and following any cybersecurity incident, system change, or regulatory update

---

3. Policy Statement

Cedric Dean Holdings, Inc. (CDH) is committed to protecting the confidentiality, integrity, and availability of all electronic systems and sensitive information, including **Protected Health Information (PHI), Personally Identifiable Information (PII), financial data, and operational records**.

This policy establishes a structured, proactive, and trauma-informed approach to **cyber risk prevention, detection, response, recovery, and continuous improvement** to safeguard program participants, employees, partners, and regulatory stakeholders.

---

4. Scope

This policy applies to:

- All CDH Peer Support NC Program systems and data
- Employees, contractors, volunteers, interns, and consultants
- Third-party vendors and Business Associates
- All electronic devices, networks, cloud services, and software platforms used for CDH operations

5. Regulatory and Standards Alignment

This policy aligns with:

- **HIPAA Security Rule (45 CFR Part 164 Subpart C)**
- **NIST Cybersecurity Framework (CSF)**
- **NC DHHS Data Security and Privacy Standards**
- **CMS/Medicaid Managed Care Requirements**
- **FTC Safeguards Rule**
- **State of North Carolina Breach Notification Laws**

6. Definitions

Cyber Attack:
Any attempt to gain unauthorized access, disrupt, damage, or steal information or systems, including malware, ransomware, phishing, denial-of-service, insider threats, or data breaches.

PHI/PII:
Protected Health Information and Personally Identifiable Information as defined by HIPAA and state law.

Incident:
Any suspected or confirmed compromise of system security, confidentiality, or availability.

7. Guiding Principles

CDH’s cybersecurity program is built on:

- **Least Privilege Access**
- **Defense in Depth**
- **Early Detection and Rapid Response**
- **Transparency and Accountability**
- **Regulatory Compliance**
- **Continuous Risk Reduction**

8. Cyber Risk Prevention Controls

8.1 Access Management

- Role-based system access
- Unique user IDs and strong password requirements
- Multi-Factor Authentication (MFA) for all administrative and remote access
- Automatic session timeouts

8.2 Device and Network Security

- Endpoint protection (anti-malware, firewall, patching)
- Secure Wi-Fi with encryption (WPA2/WPA3)
- VPN for remote access
- Prohibition of unauthorized devices (BYOD policy enforcement)

8.3 Data Protection

- Encryption of data at rest and in transit
- Secure cloud storage compliant with HIPAA standards
- Daily system backups with offsite or cloud redundancy
- Secure data disposal and media destruction

---

9. Staff Cybersecurity Training

9.1 Required Training Topics

- Phishing and social engineering awareness
- Password hygiene and MFA use
- Secure handling of PHI and PII
- Safe remote work practices
- Incident reporting procedures

9.2 Frequency

- Upon onboarding
- Annually
- After any major cyber incident

---

10. Incident Detection and Reporting

10.1 Indicators of Compromise

- Unusual login attempts
- System slowdowns or lockouts
- Unexpected file encryption or ransom notices
- Suspicious emails or links
- Unauthorized data access

10.2 Reporting Protocol

All suspected incidents must be reported immediately to:

- **Cybersecurity Coordinator / IT Administrator**
- **Compliance Officer**
- **Chief Executive Officer (or Designee)**

No employee will face retaliation for reporting in good faith.

---

11. Cyber Incident Response Plan

CDH follows a **6-Phase Response Model**:

Phase 1 – Identification

- Confirm scope and type of attack
- Isolate affected systems

Phase 2 – Containment

- Disconnect compromised devices from network
- Disable affected user accounts
- Block malicious IPs/domains

Phase 3 – Eradication

- Remove malware or unauthorized access
- Patch vulnerabilities
- Reset credentials

Phase 4 – Recovery

- Restore systems from secure backups
- Monitor for reinfection or anomalies
- Validate data integrity

Phase 5 – Notification

- Determine breach notification requirements
- Notify NC DHHS, CMS/MCOs, affected individuals, and law enforcement as required by law
- Coordinate legal counsel and compliance teams

Phase 6 – After-Action Review

- Root cause analysis
- Policy and training updates
- Corrective action implementation

---

12. Ransomware Response Protocol

CDH will:

- Not pay ransom without CEO and legal counsel authorization
- Preserve forensic evidence
- Report to law enforcement and regulatory authorities
- Activate backup restoration procedures
- Conduct breach impact assessments

---

13. Third-Party and Vendor Security

All vendors and Business Associates must:

- Sign HIPAA Business Associate Agreements (BAAs)
- Maintain cybersecurity standards aligned with NIST and HIPAA
- Notify CDH of any breach affecting CDH data within 24 hours

---

14. Data Breach Notification

CDH will comply with:

- HIPAA Breach Notification Rule
- NC Identity Theft Protection Act
- CMS and MCO contractual reporting requirements

Notifications will include:

- Nature of the breach
- Data affected
- Remediation steps
- Protective actions for impacted individuals

---

15. Roles and Responsibilities

15.1 Chief Executive Officer

- Authorizes incident escalation and regulatory reporting
- Approves cybersecurity policies and funding

15.2 Cybersecurity Coordinator / IT Administrator

- Maintains system security controls
- Leads technical incident response
- Conducts vulnerability assessments

15.3 Compliance Officer

- Ensures regulatory reporting
- Maintains breach documentation
- Coordinates audits

15.4 Workforce Members

- Follow cybersecurity procedures
- Report suspicious activity immediately

---

16. Business Continuity and Disaster Recovery

CDH maintains:

- Secure cloud backups
- Redundant communication systems
- Alternative service delivery methods for peer support operations
- Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for critical systems

17. Monitoring and Auditing

- Quarterly vulnerability scans
- Annual risk assessments
- Access log reviews
- Policy compliance audits

18. Documentation and Recordkeeping

Maintained records include:

- Incident reports
- Training logs
- Risk assessments
- Vendor agreements
- System access logs

Records are retained per CDH Records Management Policy.

19. Non-Retaliation Policy

CDH prohibits retaliation against individuals who report cybersecurity concerns or incidents in good faith.

20. Enforcement

Non-compliance may result in:

- Retraining
- Disciplinary action
- Contract termination
- Regulatory reporting when required

21. Policy Review and Revision

This policy will be reviewed:

- Annually
- After any cyber incident
- When laws, regulations, or technology platforms change

---

22. Approval and Authorization

Approved By:
Cedric Dean, Chief Executive Officer
Cedric Dean Holdings, Inc.

Signature: ___________________________
Date: January 21, 2026

---

23. Organizational Commitment Statement

Cedric Dean Holdings, Inc. affirms its commitment to **digital trust, privacy protection, and operational resilience** in service of the communities we support.