MiCT Security Policies, Standards, and Procedures

- 0. Security Program Overview
- 1. Security Architecture and Operating Model
- 2. Roles, Responsibilities and Training
- 3. Policy Management
- 4. Risk Management and Risk Assessment Process
- 5. Compliance Audits and External Communications
- 6. System Audits, Monitoring and Assessments
- 7. HR and Personnel Security
- 8. Access
- 9. Facility Access and Physical Security
- 10. Asset Inventory Management
- 11. Data Management
- 12. Data Protection
- 13. Secure Software Development and Product Security
- 14. Configuration and Change Management
- 15. Threat Detection and Prevention
- 16. Vulnerability Management
- 17. Mobile Device Security and Media Management
- 18. Business Continuity and Disaster Recovery
- 19. Incident Response
- 20. Breach Investigation and Notification
- 21. Third Party Security and Vendor Risk Management
- 22. Privacy Practice and Consent
- 23. Addendum and References
- Appendix A. Employee Handbook
- Appendix B. Approved Software
- Appendix C. Approved Vendors
- Appendix D. Key Definitions
- Appendix E. HIPAA Business Associate Agreement
- Appendix F. HIPAA Controls Mapping
- Appendix G. NIST Controls Mapping
- Appendix H. Privacy Policy
- Appendix I. Cookie Policy
- Appendix J. GDPR Data Processing Agreement