VCCCD Security Compliance Plan

Scope: To address noncompliance in areas identified by GLBA Security Audit.

3 Months (March – June 2021)

- General User (Student/Faculty/Staff) Password Management
- System Account Password Management Policy – Section 8
    - Local, Admin, Network, Service Accounts
    - NIST Standard
        - LAPS and Thychotic
- Begin to build out Internal Organizational Risk Assessment (CISOA Security Training)
- Change Management Policy
- Move to OAUTH 2.0 Standard
- Remove Legacy Email Protocols (IMAP/POP) and Forwarding

6 Months (July-September)

- MFA enabled for all employees.
- All servers upgrade to 2012 or later
    - All critical server vulnerabilities patched (end of life/catch up perspective)
- Training end users (cornerstone – Vision Resource Center https://visionresourcecenter.cccco.edu/)
- Reduce access to data from off campus by removing secure portal/desktop access

12 Months (Oct 21 – March 22)

- Build out security requests and approval workflow
- Build out Banner/Argos/Onbase permissions based on role
- DLP for Email
- Remove generic ad/student login accounts districtwide
- 100% trend micro endpoint protection on all district owned devices
- Clear Pass Training
- Onboarding and Termination account management processes
- Internal Security Audit

24 Months (March 22 – March 23

- DLP for hosts
- Vendor Management Standard
- Data Retention Strategy Rollout (Email, Network Drives/OneDrive, Onbase)
- External Security Audit