## Information Security AR Overview

1. **AR 3726: Disaster Recovery:** outlines the strategy and basic procedures to enable **NAME OF CC DISTRICT** to withstand the prolonged unavailability of critical information and systems and provide for the recovery of District Information Technology (IT) services in the event of a disaster.
2. **AR 3727: Access Control:** describes access controls to **NAME OF CC DISTRICT** sites, information and applications.
3. **AR 3728: Physical Security:** describes physical security methods that are used to protect access to IT facilities and equipment. This includes regulations for visitors to IT facilities and for the destruction of unneeded media.
4. **AR 3729: Logging and Monitoring:** outlines the requirements for IT infrastructure logging and monitoring for potential security incidents at**NAME OF CC DISTRICT**. Logging relates to the automatic recording of events and metrics generated by hardware and software. These logs can be useful in intercepting security breaches for they can cause damage.
5. **AR 3730: Remote Access:** describes access controls to **NAME OF CC DISTRICT** information and systems from remote (offsite) locations.
6. **AR 37xx: Acceptable Use:** outlines the acceptable use of electronic assets at **NAME OF CC DISTRICT**. This is based on our need to comply with ISO 27002 standards and PCI-DSS requirements.
7. **AR 37xx: Change Control:** outlines a standardized method for handling changes to district-wide data infrastructure and associated software.
8. **AR 37xx: Data Classification:** outlines information security requirements for ownership, classification, and protection of district-wide information assets.
9. **AR 37xx: Information Security Program Overview:** Overview of the district-wide Information Security program.
10. **AR 37xx: Network Security:** describes network controls required to protect **NAME OF CC DISTRICT** information and systems.
11. **AR 37xx: Secure Operations:** describes a set of practices to promote the secure operations of **NAME OF CC DISTRICT** information and systems including: Operations Processing, Virus Management, Patches and Updates, Backup, Third Party Management.
12. **AR 37xx: Security Incident Response:** describes requirements and procedural steps to enable a quick and effective recovery from unplanned **NAME OF CC DISTRICT** security incidents.