Appendix F: Security Requirements

Infrastructure

- AURA utilizes both wired and wireless network infrastructure.
    - In cases of wired connectivity, it is desirable for a device to support 802.1x authentication for port security.
    - Wireless devices should also support 802.1x authentication, and WPA2-Enterprise is required.
- DHCP or fixed IP addresses can be utilized, depending on the requirements.
- Ideally, the refreshed equipment would be assigned to a dedicated network segment (security zone) specifically reserved AV functionality/support.
- Guest connectivity should be avoided due to the reduced monitoring and lack of control over the connected devices.
- 1Gb service ports are typical. 10Gb ports are available in the data centers.
- Server-based components should be deployed to the datacenter or similarly-secured areas to avoid the risk of tampering. Portable racks should be locked and secured appropriately.

Cloud-Based Components

- Depending on the type of data being consumed or released, cloud-based components, platforms, etc. may require FedRamp approval. This is generally evaluated on a case-by-case basis.

Encryption Requirements

- AURA is required to utilize FIPS140-2 compliant cryptographic components.
- Traffic to and from devices - especially web traffic - is required to be encrypted. This includes data streams over TLS, etc. AURA provides certificate infrastructure and can issue certificates for web interfaces.
- Management interfaces should also be similarly configured. HTTP is not allowed (see hardening section below)

Authentication

- When possible, SSO-based or AD domain-based authentication should be required.
- SSH, web, management interfaces should all use domain-based accounts, and access should only be granted on an as-needed basis.
- "Break-glass" accounts are allowed, but should be individual to each service and device, and an approved password management solution should be utilized to manage these credentials.
- Staff should always utilize domain-based accounts for day-to-day work. Break-glass accounts are to be used only when needed to recover, reset a device, etc.
- SSH keys should be treated like passwords and rotated per AURA requirements, with staff changes, etc.

Hardening

- Check with vendors to see if a security hardening guide is provided with each component. This is especially important with appliance-based products.
- More general components (such as in-house built servers) should use AURA-hardened configurations (CIS benchmarks).
- A baseline configuration/build sheet should include steps taken to inspect and harden devices.
- Ensure devices are running the latest supported code, firmware, etc.
- AURA should provide NTP for time sync.

Maintenance and Vulnerability Management

- Review the vendor's patch release schedule, notes, etc. to ensure there is evidence of due diligence and due care. Dated or non-existent patch releases may be a red flag.
- Vendors usually provide patch or maintenance procedures and plans. These should include software and firmware updates if the product is appliance-based.
- Market research should be completed on the vendor and supply chain components for evidence of past vulnerability management, security incidents, etc.