University Information and Technology Services (UITS)

February 1, 2018

CRITERIA AND PROCESS FOR PRIVILEGED ACCOUNT ACCESS

Privilege Account Access will be granted if all of the following criteria are met:

- The user needs to perform CSU official business and be a full-time employee.
- Approval by your immediate supervisor (department manager, director, chair, dean or vice president).
- An eQuest has been submitted to UITS requesting grant and approval of Privilege Account.[1]
- The user is performing work on CSU-owned hardware or software.
- The user has completed the yearly CSU Security Awareness Training.
- The user's ***level of access*** to the Privilege Account will be determined by the USG Policy of Least Privilege (PoLP) from the USG IT Handbook. The IT Management Section 3 states, "The Principle of Least Privilege (PoLP) describes minimal user profile or access privileges to information resources based on allowing access to only what is necessary for the users to successfully perform their job requirements."

Privileged Account Access will NOT be granted:

- For personal use.
- For purposes of installing non-CSU purchased or approved software. User must follow the current UITS software vetting and CSU purchasing processes that includes approval by VP of IT/CIO. (See Software Vetting Process).
- For purposes of installing open source (free) software that poses possible high security risk of infection and has not been reviewed, vetted and approved via a UITS technician and Chief Information Security Officer (CISO). (See Software Vetting Process).
- If no specific details pertaining to the operation or task are listed in the eQuest description field. The details will be used for security auditing purposes. For example: use of peripherals and hardware, specific software, specific updates, and etc.

Condition of Use of Privileged Account Access Off-Campus

- In circumstances where users are requesting Privileged Account Access for the purpose of attending conferences, off-campus training, and other activities off-campus, the level of access may be determined and/or restricted on a case-by-case basis at the sole discretion of the CIO or CISO.
- Connections made via ***free, public*** wi-fi access are extremely vulnerable to malware and data breaches and are strongly discouraged. Employees connecting in such a manner may be held responsible for security breaches by having their Privilege Account Access suspended or revoked.
- Users are strongly encouraged to connect off campus via Virtual Private Networks (VPN) or wi-fi access that is purchased from a reputable telecom carrier.

---

[1] The eQuest Description Field must provide a detailed description of the reasons underlying the request for Privileged Account Access.

Software Vetting Process:

1. Submit an eQuest to UITS Technology for Software under the Office Equipment category.

2. EQuest will be reviewed by UITS Technology Procurement Consultant, Desktop Support Manager, and, if necessary, CISO within 48 hours after the eQuest has been assigned.

3. If the CSU owned licensed software has been approved, the installation will be within 24 hours following approval.

4. If the non-CSU owned licensed software has been approved, the CSU purchasing process must be followed. The purchasing process time will vary based on factors such as vendor and software manufacturer.

5. If the open source (free) software has been approved, the installation will be within 24 hours following approval.