Southern OREGON UNIVERSITY

Multi-Factor Authentication Proxy

Office: Information Technology
Procedure Contact: Infrastructure Services Manager
Related Policy or Policies: Multi-Factor Authentication

Revision History

Revision Number:	**Change:**	**Date:**
1.0	Initial Version	**November 2018**

A. Purpose

To establish an efficient and secure process for granting vendors remote access to SOU assets.

B. Definitions

1. Multi-factor Authentication - An additional layer of security added to any type of account, requiring extra information or a physical device to login, in addition to a password.

2. A Multi-factor Authentication Proxy (MFA-Proxy) is a SOU employee that can act a proxy for the IT department to create MFA tokens in order to grant temporary access to SOU systems/resources. To have MFA-Proxy authority, a formal request must be made to IT specifying:
   a. the person to act as the proxy
   b. the system(s) where access will be needed
   c. a description of the type of work to be performed by the external provider
   d. a signature confirming:
      i. the understanding of involved risks
      ii. accepting responsibility for vendor/consultant actions
      iii. proper management of the tokens as described in this procedure

3. A Multi-factor Authentication token (MFA-token) is a qualifying physical device used to satisfy the requirements of Multi-factor Authentication, such as a landline phone, a smartphone with an MFA enabled app, or a physical token such as a USB device.

C. Procedures

1. MFA-Proxy rights are granted by the Infrastructure Services Manager, contingent upon a review of the aforementioned request and a background check.

2. The CIO can choose to waive the requirement for a background check if a background check is current or for other reasons.

3. The MFA-Proxy will be given the username and password of the provider's generic account.

4. A special MFA-token will be configured by IT for the MFA-Proxy on the vendor account that will enable them to manage MFA-tokens for their external provider.

5. When a vendor employee needs to use the account, the MFA-Proxy will add a MFA-token for the vendor employee.

6. After the vendor employee has completed their work for the University, the MFA-Proxy will revoke the MFA-token from the vendor employee.

7. IT will periodically audit vendor generic accounts. The MFA-Proxy will be required to explain the presence of MFA-tokens on a vendor generic account.

This procedure may be revised at any time without notice. All revisions supersede prior procedures and are effective immediately upon approval.

D. Appendix

IT reserves the right to revoke MFA-Proxy privileges at any time without notice.