User Management Polices

Tyler D Lown

Oregon Institute of Technology

4/30/2021

Author Note

This policy and procedures document was written for the client Westlake Realty Group and Dr Erin Pumroy of WRI327

Table of Contents

[**Summary:** 3](#_Toc71313410)

[**Introduction:** 4](#_Toc71313411)

[**3. User Management Security Policies** 5](#_Toc71313412)

[**3.01 Policy: Onboarding users** 5](#_Toc71313413)

[**Procedures:** 6](#_Toc71313414)

[**3.02 Policy: Requesting Edits to User** 7](#_Toc71313415)

[**Procedures:** 7](#_Toc71313416)

[**3.03 Policy: Request for Software Download** 9](#_Toc71313417)

[**Procedures:** 9](#_Toc71313418)

[**3.04 Policy: User Password Reset Requests** 10](#_Toc71313419)

[**Procedures:** 10](#_Toc71313420)

[**3.05 Policy: Offboarding a User** 11](#_Toc71313421)

[**Procedures:** 12](#_Toc71313422)

[**Conclusion:** 13](#_Toc71313423)

[**Additional Information:** 13](#_Toc71313424)

# **Summary:**

This policy and procedures give the support staff information necessary to uphold the security standards for the organization. This document covers the 5 policies in the following order: Onboarding users, requesting edits to users, requesting for software downloads, user password reset requests, and finally offboarding user. These five policies must be followed by all employees of the organization and applied by the support staff members.

**Introduction:**

A safe and secure online environment is a vital part of doing business for most businesses today, but developments in technology require a constantly updated set of guidelines. Creating guidelines is a useless task unless everyone and everything on the computer network is compliant with these standards. Informed users are arguably just as important as compliant devices and because of that requires just as much attention as most parts of the Information Technology (IT) infrastructure. This document will review existing user management policies and procedures that have been updated as well as new implementations that introduce modern security features.

This document is one part of a series of policies intended for IT Support staff members' use. Figure 1 below identifies the different categories of IT policies based on the policy number. The corporation provides these policies and procedures for guidance so that security standards are met to the fullest. These policies and procedures apply to all employees of the organization.

Figure 1. Support Staff Categories of IT Policies

**3. User Management Security Policies**

Figure 2. User Employment Process

**3.01 Policy: Onboarding users**

This policy is intended to ensure that all new employees go through the complete onboarding process and tasks that are performed are documented for historical referencing. The corporation requires all new onboarding processes to utilize the procedures below to best ensure user and business security. An onboarding request must be submitted by using the IT Onboarding documents in the IT folder on the company SharePoint.



Figure 3. Sample Onboarding Document.

**Procedures:**

The following procedures will direct the support staff on how to onboard a new user with the details in the onboarding document.

**3.01.1 Verifying an Onboarding Request**

Verify the onboarding document used is the most current version available on SharePoint.

Each department must have a designated manager or supervisor who can approve onboarding requests.

Ensure the document has all the information to onboard the new user as well as a signature provided by the designated manager or supervisor.

**3.01.2 Processing an Onboarding**

All onboarding requests must have a corresponding support ticket to maintain details.

Use details in the onboarding document to create new accounts and profiles, add licensing, and apply access rights.

Increases in cost or changes in billing must be sent to accounting.

All changes must be recorded in the ticket notes.

User credentials and login information must be sent using an encrypted email message.

**3.01.3 Recording onboarding request**

After onboarding is complete, the file needs to be saved in the IT UserData subfolder inside the IT Department folder on the company SharePoint.

File naming convention must identify the user and then the date. See Figure 4 below for an example.



Figure 4. Onboarding/Offboarding File Naming Convention

**3.02 Policy: Requesting Edits to User**

This policy is designed to ensure that requests are properly processed and documented for edits made to a user’s account. Utilizing the procedures of this policy is required when receiving an edit request form to best provide security and auditing capabilities.

User Edit Request forms must be completed or signed by authorized designated staff members.

**Procedures:**

Any requests to add or remove access to software, resources, hardware, or to change users’ details must follow this policy.

**3.02.1 Verify Edit Request**

Ensure the User Edit Request document is the most current version available.

Only designated managers and supervisors can authorize edits.

Validate that the requester is authorized or that an authorized signature is on the requesting document.

**3.02.2 Processing edit Requests**

All changes must have a matching support ticket for historical details.

Use the edit request document to make the edits on the designated account.

Changes in billing or price must be sent to accounting.

All changes and additions must be records in the support ticket notes.

User credentials and login information must be sent using an encrypted email.

A sample edit request form can be seen In figure 5 below:

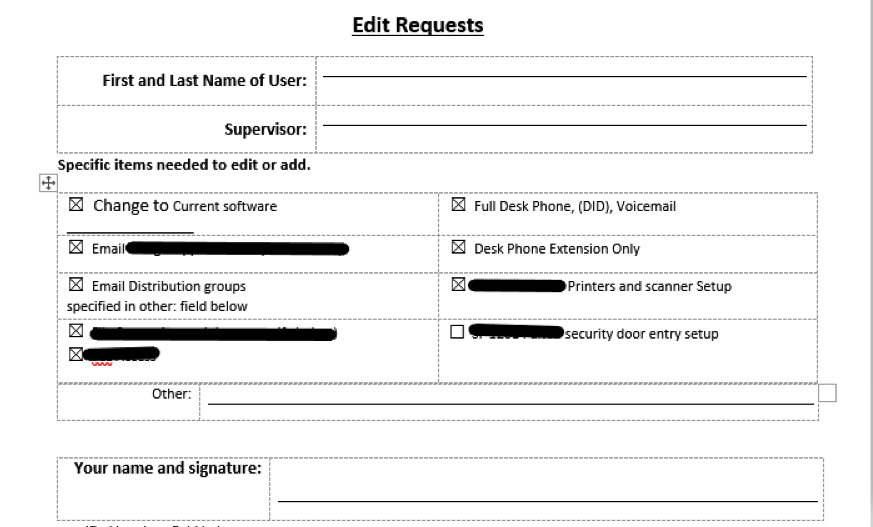


Figure 5. User Edit Request Form Sample

**3.02.3 Recording Edit requests**

After changes are complete, the edit request document must be attached to the end of the user onboarding document in the IT UserData Subfolder inside of the IT folder on SharePoint.

**3.03 Policy: Request for Software Download**

The purpose of this policy is to ensure verification and documentation of the individual requesting access to the software. The overall goal is to ensure proper licensing and access is provided to only the individuals that have the permission to do so.

**Procedures:**

Any request for access to corporate-owned software and is part of the list documented software must adhere to this policy.

**3.03.1 Verifying a download request**

A request for a download link can only be requested by the user or a designated ranking staff member.

A user needs to have the licensing and software assigned in the onboarding document. If not, an edit request should be made prior.

**3.03.2 Processing a download request**

Any download request must also have a ticket to retain information about related processes.

for on-premise workstations, support staff needs to install the software using administrative credentials.

For remote users, a download link can be installed by the user or over a remote screen-share session.

Server installations must be performed or approved by an IT manager.

**3.03.3 Recording a download Request**

All changes must be documented before closing the ticket.

**3.04 Policy: User Password Reset Requests**

This policy is intended to guide support staff whenever a request to reset a user’s password on any account or profile is received in any communication form. The objective of this policy is to ensure that password reset requests are authentic and the requester is authorized.

**Procedures:**

Any request to reset software for a user account must follow this policy to ensure organizational security.

**3.04.1: Verifying a password reset request**

If a request is from an unknown personal account, call the user on the phone to verify the request.

Only the user and their manager can request a password reset.

Confirm which account or profile the user is unable to log in to.

**3.04.2: Processing a password reset request**

Reset requests need a ticket created to maintain historical information.

Any password reset request that involves giving the user a temporary password must be followed by the user resetting the password.

Messages that contain credentials or account information must be sent with an encrypted email message.

Task completed during a password reset needs to be documented in the ticket notes.

User confirmation of resolution will be notated in the ticket notes before closing.

**3.05 Policy: Offboarding a User**

This policy was created to provide the support staff with guidance when an offboarding request is received. This policy is required when an offboarding request has been sent to the support staff to ensure that a user does not have access after the fact.

Offboarding requests can only be submitted or approved by designated managerial or supervisory roles.

A sample offboarding document can be seen in figure 6 below:

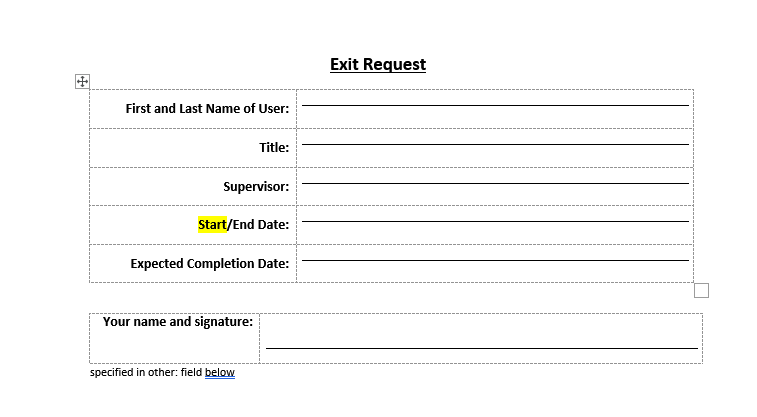


Figure 6. User Exit Request Form

**Procedures:**

Requests made to offboard a user from the organization and remove complete access must comply with this policy.

**3.05.1 Verifying Offboarding requests**

Ensure the offboarding request document is the most current version available.

Verify that the offboarding request is sent by or contains the signatures of the designated staff member.

**3.05.2 Processing offboarding Requests**

An offboarding ticket must be created each time an offboarding request is made to document what tasks were completed and when.

The onboarding document must be used to roll back any changes made during the length of employment.

All electronic user accounts need to have the password reset and login disabled.

**3.05.3 Recording offboarding requests**

After the offboarding process is complete, the offboarding request needs to be attached to the end of the user's full onboarding document.

With the offboarding request attached, **move** the file from the User Onboard subfolder into the User Offboard inside of the IT department folder in SharePoint.

Must report completion to the requestor once the offboarding process is complete.

**Conclusion:**

Users will always be part of an organization and require attention just as most components of the IT infrastructure. Having thorough guidelines for incoming and outgoing user can be crucial for preventing unnecessary breaches. These policies and procedures are intended for the support staff to have clear and easily accessible information about the various parts of IT management such as managing users. This document is one part of a series of three that explain the policies and procedures in place for the different areas of the IT infrastructure. Following these guidelines will ensure that the process of managing users is done so with security always in mind.

**Additional Information:**

For emergencies, Contact the IT manager at 541-591-XXXX or go to https://www.labtech.lightspXXXX.com:8040/

Hardware and software management policies can be accessed in the **IT Support training folder**.