

SharePoint External User Policy

1.0 Overview

SharePoint is a secured collaboration platform for customized Web services. It is used by JWB primarily to share information internally and externally among staff, partners and funded agencies. This data can include confidential data, including client identifying information. Therefore, it is imperative to ensure that proper security policies are in place to protect the integrity of the data.

2.0 Purpose

The purpose of the SharePoint External User Policy is to establish the rules for the creation, monitoring, control and removal of SharePoint user accounts.

3.0 Scope

The scope of this policy covers all individuals with authorized access to any JWB SharePoint site. This policy applies not only to employees, but also to guests, contractors, and anyone requiring access to the organization's SharePoint site.

4.0 Policy

4.1 Account Setup

During initial account setup, certain checks must be performed in order to ensure the integrity of the process. The following policies apply to account setup:

- Appropriate written authorization must be obtained prior to establishing accounts and access including the submittal of the SharePoint User Access form.
- Completed forms should be submitted to the appropriate JWB Contact. The JWB Contact will then submit the form to the JWB Help Desk.
- Users will be granted the least amount of access required to perform his or her job function based on the Principle of Least Privilege
- Users will be granted access only if he or she accepts the SharePoint External User Policy.
- All user accounts must be uniquely identifiable using the assigned user name.
- If a user currently utilizes a Microsoft 365 Account for Business, guest access may be granted using the user's organization email to gain access to SharePoint.
- User passwords must be constructed in accordance with the JWB Password Policy.
- Access to the network will be granted in accordance with the Acceptable Use Policy.
- Providers and partners in conjunction with contract management staff are responsible for determining who at the provider or partner agency has access to their individual SharePoint sites.

4.2 Account Termination

When a user is terminated, JWB must be notified within 3 days of termination.

4.3 Account Use

Network accounts must be implemented in a standard fashion and utilized consistently across the organization. The following policies apply to account use:

- Accounts must be created using a standard format (i.e., firstinitiallastname)
- Accounts must be password protected (refer to the Password Policy for more detailed information).
- Accounts must be for individuals only. Account sharing and group accounts are not permitted.
- Providers and partners are responsible for monitoring user accounts for their individual sites. A periodic review should be conducted to monitor access.
- Users no longer having a business need for access to the sites should have access removed by contacting JWB.
- JWB will review SharePoint access every six (6) months. Accounts that have not been logged into within six (6) months will have access to the system terminated. A new form will need to be completed to restore access.

4.4 Use of Passwords

When accessing the SharePoint network, a username and password is the only acceptable means of authentication. Passwords must conform to JWB's Password Policy as follows:

- Passwords should be at least 12 characters. The longer the password is, the more secure it will be
 - Password must contain characters from three of the following four categories:
 - English uppercase characters (A through Z)
 - English lowercase characters (a through z)
 - Base 10 digits (0 through 9)
 - Non-alphabetic characters (for example, !, \$, #, %)
- Passwords must not be comprised of, or otherwise utilize, words that can be found in a dictionary
- Passwords should not be comprised of an obvious keyboard sequence (i.e., qwerty)
- Passwords should not include "guessable" data such as personal information like birthdays, addresses, phone numbers, locations, etc.
- Passwords should not contain the user's account name
- Repeated patterns in passwords should be avoided (i.e., P@\$\$w0rdJan21, P@\$\$w0rdApr21, P@\$\$w0rdJul21)

Complexity requirements are enforced when passwords are changed or created.

4.5 Multi-Factor Authentication

Multi-factor authentication will be activated on all JWB accounts. Users must provide a cellphone number or install the Authenticator App on a mobile device to receive a code to log into the JWB

network. Codes may be received through text message, phone call, or the Authenticator App. The use of an office number is discouraged since this method of verification may not always be accessible. The use of personal email addresses (Gmail, Yahoo, AOL, etc.) for authentication to JWB's SharePoint sites is prohibited.

4.6 Confidentiality

Passwords should be considered confidential data and treated with the same discretion as any of the organization's proprietary information. The following guidelines apply to the confidentiality of organization passwords:

- Users must not disclose their passwords to anyone
- Users must not share their passwords with others (co-workers, supervisors, family, etc.)
- Users must not write down their passwords and leave them unsecured
- Users must not check the "save password" box when authenticating to applications
- Users must not use the same password for different systems and/or accounts
- Users must not send passwords via email
- Users must not re-use passwords

4.7 Change Frequency

In order to maintain good security, passwords should be periodically changed. This limits the damage an attacker can do as well as helps to frustrate brute force attempts. At a minimum, users must change passwords every 90 days.

4.8 Incident Reporting

Since compromise of a single password can have a catastrophic impact on security; it is the user's responsibility to immediately report any suspicious activity involving his or her passwords to JWB. The Incident Response and Breach Notification Procedures must be implemented as appropriate.

4.9 Failed Logons

Repeated logon failures can indicate an attempt to 'crack' a password and surreptitiously access a network account. In order to guard against password-guessing and brute-force attempts, JWB must lock a user's account after 3 unsuccessful logins. This can be implemented as a time-based lockout or require a manual reset, at the discretion of IT.

In order to protect against account guessing, when logon failures occur the error message transmitted to the user must not indicate specifically whether the account name or password were incorrect. The error can be as simple as "the username and/or password you supplied were incorrect."

Additionally, users accounts will be locked for 15 minutes after 3 unsuccessful attempts are made to enter the validation code for Multi-Factor Authentication. Additionally, users can report unsolicited codes as fraud by replying to the text message with the number "0". This will subsequently lock the account and report the attempt to IT. Users should also report unsolicited codes to IT.

4.10 Applicability of Other Policies

This document is part of JWB's cohesive set of security policies and procedures. Other policies or procedures may apply to the topics covered in this document and as such the applicable policies and procedures should be reviewed as needed.

4.11 Implementation Guidance

- Users must not attempt to access any data or program contained on the JWB SharePoint site for which they do not have authorization or explicit consent.
- Users must not purposely engage in activity that may: harass, threaten or abuse others; degrade the performance of SharePoint and related IT property; deprive an authorized user access to a SharePoint resource; obtain extra resources beyond those allocated; circumvent SharePoint security measures.
- Users must not download, install or run security programs or utilities that reveal or exploit weaknesses in the security of SharePoint and related IT property, unless directly said in job purpose.
- SharePoint can only be used for sharing information with JWB. It may not be used for any other business purposes.
- SharePoint must not be used for personal benefit.
- Users must not intentionally access, create, store or transmit material on the SharePoint which JWB may deem to be offensive, indecent or obscene.
- Users must not otherwise engage in acts against the aims and purposes of JWB as specified in its governing documents or in rules, regulations and procedures adopted from time to time.
- All messages, files and documents – including personal messages, files and documents – located on SharePoint are owned by JWB, may be subject to open records requests, and may be accessed in accordance with this policy.

5.0 Enforcement

This policy will be enforced by the JWB assigned Security Officer, IT and the Executive Team.

6.0 Revision History

Revision 1.0, 9/12/2013
Revision 2.0, 11/13/2014
Revision 3.0, 3/1/2019
Revision, 4.0, 3/1/2020
Revision, 5.0, 3/1/2021
Revision, 6.0, 3/2023