Multi-Factor Authentication Core User Policy and Procedures

Core Users with access to other people’s sensitive or restrictive information must use one-time passwords (OTP) generated from approved fobs or smartphone OTP apps in addition to their campus credentials to access UW System common systems that require multi-factor authentication.

This document specifies Core User responsibilities and procedures when using these fobs or smartphones. It is organized in these sections:

1. Policy
2. Procedure/Processes
3. Background Information
4. Definitions
5. Authorization Form

Policy

1. All Core Users must use the generated OTPs from approved fobs or smartphone OTP apps as second factor in addition to their campus credential to authenticate to UW System common systems that require multi-factor authentication.
2. Devices that are used to generate OTP cannot be used to authenticate to UW System common systems that require multi-factor authentication. As such, tablets, desktops and other large screen devices are not allowed.
3. Users who only have the following access are excluded from the multi-factor authentication effort:
   a. Manager self-service for Time and Labor/Absence Management
   b. Employee self-service for time reporting
   c. Talent Acquisition Management
   d. eBenefits

Procedure/Processes

Every Core User must choose to use either fob or smartphone as the OTP device, but not both. Both fob and smartphone OTP app will be supported by UW Digital ID. If a Core User chooses to use a smartphone to generate OTP, he/she is responsible for providing his/her personal smartphone or a State-issued smartphone (if a user already has state issued smartphone). The UW-System will not issue smartphones just for Core Users to use as multi-factor authentication devices.

UW-System is not responsible for the cost of repairing or replacing the personal smartphones that are used as OTP devices or for the data plan.
1. **Device Options**

Each Core User can choose a fob or a smartphone based on their work/life style and preference. It is a personal choice.

   a. **Fob:**
      
      i. **How to use it?**
         1. Each fob comes with a hole on the device for key ring.
         2. A Core User will need to press a button on the fob to generate an OTP
      
      ii. **Pros:**
         1. Fobs are free of charge for Core Users.
         2. Fobs are State-issued devices; therefore, if there are issues with fobs, Core Users can seek help from their campus Local Registration Authorities (LRAs).
      
      iii. **Cons:**
         1. The fob is an additional device that Core Users have to remember to carry if they need to authenticate to UW System common systems that require strong authentication.
      
      iv. **Fob User Responsibilities:**
         1. Core Users are expected to return their fobs to their campus LRA when they terminate their affiliation with UW-System.
         2. Core Users are expected to return their fobs to their campus LRA when they no longer have Core User roles to any of the UW System common systems that require multi-factor authentication.
         3. Currently Core Users will not be charged for lost fobs. However, this policy may be changed in the future. Core Users must take reasonable care for the fobs that are assigned to them. Reasonable care includes, but is not limited to:
            a. Not putting their fobs through washers or under the water on purpose. These fobs are not water resistant.
            b. Protecting from loss or theft
            c. The Core Users are expected not to store their OTP fobs in the same office or near a computer used to access the HRS.
            d. The Core Users are expected not to transport their OTP fobs in the same bags as laptops that are used to access the HRS.

OR
b. Smartphone
   i. How to use it:
      1. Core User must install an OTP app from Symantec
      2. Core Users use the installed OTP app to generate OTP.
   ii. Pros:
      1. Smartphone Core Users do not have additional devices such
         as fobs to remember to carry with them in order to
         authenticate to UW System common systems that require
         strong authentication.
      2. The usage of OTP app is free of charge to Core Users.
   iii. Cons:
      1. Depending on user’s smartphone contract, there may be a
         fee associated with using the internet to download the OTP
         app initially.
      2. UW Digital ID only supports the OTP app, not the
         smartphone itself. Core Users are responsible for making
         sure that their smartphones are in working condition.
   iv. Smartphone User responsibilities
      1. Core Users are expected to leverage to electronic security
         provided by their smartphones to access their smartphones
      2. Core Users must notify their campus LRA when they change
         their smartphone device even if they keep the same phone
         number.

2. Common Procedures and Processes:
   a. Core Users are expected to use the chosen device in addition to their
      campus credential to authenticate to UW System common systems that
      require strong authentication on a regular basis. Currently there is no limit
      on how many times a Core User can request a temporary OTP. However,
      UW System monitors the pattern of contingency access usage and may
      also issue a report to the supervisor of a Core User if the Core user
      request temporary OTP more than five times in a month.
   b. Contingency Access
      Core Users are able to use either one of the following options to request
      temporary one-time passwords when they don’t have their OTP device to
      authenticate to UW System common systems that require strong
      authentication:
i. Login to contingency access website (https://uwdigitalid.wisconsin.edu/index.php?p=27) to request a temporary OTP: Core Users can access the website 24 hours a day, 7 days a week.

Note that if a Core User chooses to receive the temporary OTP through text message, depending on user’s smartphone contract, there may be a fee associated with each OTP text message. Core Users are responsible for paying for these text message fees.

ii. Seek help from campus LRA: Core Users can seek help from their campus LRAs during campus LRA’s defined business hours.
   c. Core Users are expected notify their LRAs when their roles are been changed to non-Core User roles.
   d. Core Users are expected to notify their campus LRAs when they terminate their affiliation with UW-System.
   e. Core Users are expected to report lost or damaged device to their campus LRA during campus LRA’s defined business hours.
   f. Core Users must take responsible care of their OTP devices. This includes, but is not limited to:
      i. Core Users are expected not to leave their OTP devices unattended in a public place.

Background Information

With technology advances and new emerging threats that we face, we have an increased responsibility to provide additional security measures to ensure that the data we collect, consume, and store is secure from unauthorized access. UW-System has developed a stronger method for users to sign into or logon to UW-System apps that store and process restricted and sensitive data. This effort is known as the Multi-Factor Authentication project.

One-Time Passwords (OTP) has been selected as the technical platform to address multi-factor authentication. An OTP is valid for only one login session. The OTP platform requires the user to use either a fob or a smartphone that is synchronized with a server to generate the password. All Core Users are required to use the generated OTPs as second factors in addition to their campus credentials to authenticate to UW System common systems that require strong authentication.

Definitions
<table>
<thead>
<tr>
<th>Term, Abbreviation or Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fob</td>
<td>A State-issued device that is used to generate One Time Password.</td>
</tr>
<tr>
<td>Core User</td>
<td>These are employees who authenticate to through the web interface and who can access other people’s sensitive or restrictive information in order to perform their job duties.</td>
</tr>
<tr>
<td>LRA</td>
<td>Local Registration Authority. The OTP LRAs are responsible for identity proofing Core Users when provisioning fobs to users.</td>
</tr>
</tbody>
</table>
| Multiple-Factor Authentication | Authentication containing at least two of the three quality mechanisms:  
Something a person “knows” – Passwords, PIN numbers, passphrases, a secret handshake, and mother’s maiden name.  
Something a person “has” – Identity badges/cards, physical keys, a driver’s license, unique uniform, and digital certificates.  
Something a person “is” – These authenticators, called biometrics, are based on a physical characteristic of a person, such as fingerprint, voice pattern, retinal pattern, or facial recognition. |
| OTP:                         | One Time Password |
| OTP Device:                  | The device that is used to generate One Time Password. This reference both Fob and Smartphone |
| Smartphone OTP App          | A smartphone app that is used to generate OTP |
Authorization Form

SIGN AND TURN IN:

I have read and understand the Multi-Factor Authentication information above. I agree that I will take reasonable care of the OTP device I choose to use and follow the user responsibility requirements. I acknowledge that this form will become a part of my permanent personnel file.

Print Name: _____________________________________________

Signature: _______________________________________________

Date: ________________

Return this signed form to the human resources or LRA who gave it to you.