IRIS Multifactor Authentication Introduction

The following provides answers to frequently asked questions related to IRIS multifactor authentication (MFA) requirements and processes. Please consider the following as you prepare for your organization's IRIS use.

WHAT IS MULTIFACTOR AUTHENTICATION (MFA)?

MFA is a secure login process that requires a user to verify their identity using two or more factors before gaining access to a system. For IRIS, this means that a user will need an authenticator app (e.g., Duo, Google Authenticator, or Microsoft Authenticator) downloaded to their mobile device (i.e., cell phone or tablet) in addition to their IRIS login credentials (username and password) and a computer.

WHY DOES IRIS REQUIRE MFA?

IRIS is committed to ensuring we protect sensitive referral information, and a key aspect of this responsibility is compliance with the most current data security frameworks. Based on these standards, a single password is no longer a sufficient defense against modern cyber threats.

HOW DO STAFF SET UP MFA?

New IRIS users will complete a one-time setup using the authenticator of their choice upon their first log in and will be required to enter a verification code generated by that authenticator once each week following. For further guidance on setting up MFA, please see the **Setting Up Multifactor Authentication** guide. Gudiance for setting up your MFA connection is also available **in Spanish**.

HOW DO STAFF LOG IN USING MFA?

After setting up the connection between their chosen authenticator app and IRIS, users will only need to authenticate once per business week or after clearing their browser's cache. For all other logins during the same business week after a user has authenticated their account, they will only need to enter their IRIS username and password. See **Logging into IRIS** for further details.

ADDITIONAL WORKFLOW CONSIDERATIONS

Below are some potential instances that may impact an established MFA connection.

Cache-Clearing

If you clear your cache during the same work week in which you have already authenticated your account using the 6-digit code provided by your authenticator app, you will need to authenticate a second time.

New Browser

If you log in to a different web browser during the same work week in which you have already authenticated your account, you will need to authenticate a second time.

New Devices

If you get a new mobile device (i.e., a cell phone or tablet), you will need to complete the MFA setup process again with the new device. Your MFA connection is tied to the mobile device you originally used for setup, and if you no longer have that device, your MFA connection becomes invalid. Please reach out to IRIS Support (**irisadmin@ku.edu**), who will assist you with resetting your MFA connection.

WHAT IF STAFF DON'T HAVE A MOBILE DEVICE?

If staff don't have access to work-issued phones or aren't comfortable using a personal mobile device to manage their IRIS MFA connection, they can use a hardware key instead. The decision to implement hardware keys should be made by your organization. For more information on hardware keys, please see the **Multifactor Authentication Hardware Key FAQ**.

The IRIS Support Team can offer only limited troubleshooting for hardware keys. This means staff who reach out to IRIS Support (**irisadmin@ku.edu**) requesting assistance downloading, accessing, or troubleshooting their hardware key will be redirected to their organization's IT Department for further support.

WHAT INFORMATION DOES OUR IT DEPARTMENT NEED?

We recommend connecting with your IT Department and discussing best practices for internal application adoption during your onboarding into IRIS. You can use the below language to kick-start the conversation with them. The IRIS Support (**irisadmin@ku.edu**) Team can directly connect with your IT Department as needed.

*Our staff will use **IRIS** to coordinate community referrals for our clients. All staff within our organization who use IRIS will be required to authenticate using TOTP (Time-based One-Time Password) method once each business week using a secondary device. The only external requirement is a secondary device with a downloaded authenticator app. There are no requirements for VPN, SSO, or other admin tools. If staff are unable to use a mobile device, our organization can provide any external hardware key compatible with TOTP for their use (e.g., a Yubico Yubikey 5C).*

- *Are there any concerns or steps necessary as they pertain to our IT Department's standards?*
- *Will needing two devices to log in be a barrier for staff?*
- *Are staff allowed to use personal devices for MFA, or do they have assigned devices? Are they able to use their work device to download an authenticator app?*

- *What questions would you like answered before MFA is required within our organization?*