SoIC Account Security Recommendations

IU maintains a secure computing environment requiring things like 15+ character passphrases and passphrase resets every 2 years. There are also some additional security measures you can implement that are either required or recommended for everyone at the school. This page provides details on how you can enable these security features.

Account Login Activity Monitoring

UITS manages login records for your account. We encourage you to go to the Login Activity & Subscription Options Page and check out the options there. If you are not frequently logging into IU systems from outside of the US we strongly recommend you enable this option:

- **Send emails for non-US logins** - If you select 'Yes', you will receive notices when your account is logged in from a non-US location.

If you want to keep closer watch on all logins to your account, then you can enable this option:

- **Send Daily Emails** - If you select 'Yes', you will receive daily notices about your login activity.

If you select either of these options, please do not select the option to CC departmental IT staff

CAS+Duo Support

Anyone using secure IU systems will already be familiar with the use of 2-factor authentication using Duo. However, it is possible for all IU users to set up 2-factor authentication for all CAS logins and we encourage you to set that up. The idea is that you have some 2nd authentication method in addition to your passphrase that is needed to login. For most people, that will be an app on your phone but there are several other options.

Through the use of 2-factor authentication, if your username and passphrase were compromised it would not be possible for someone else to CAS authenticate as you without a second form of authentication. Furthermore, if someone did try to use your passphrase you might be immediately notified so you can reject the connection and change your passphrase. We view this as a critical part of securing your IU account.

The process of setting this up involves 2 steps:

1. Set up Duo 2-factor authentication per the Duo KB page
2. Once you have Duo set up and working, you can enable it for all CAS logins per At IU, how can I use CAS + Duo Authentication?. Just go to the CAS+Duo Authentication Page and enable or disable it but you are encouraged to read the CAS+Duo KB Page page before enabling it so you understand the precautions detailed there. Once you turn this on, all of your CAS authentications will require your passphrase and Duo authentication.

Email Encryption and Digital Signing

If you use the IU Exchange system, we recommend you set up the ability to send encrypted email as well as digitally signed email. Note that digitally signed messages are **NOT** encrypted in any way but it does provide a way for the recipient to verify that the email was actually sent by you and not some spammer/imposter which might be the case in a phishing scam. The SoIC recommendations are as follows for all IU Exchange users:

- Set up digital signing of all email you send as the default
- If you must email sensitive data as part of your job, it **MUST** be encrypted.

The following pages describe the process of setting this up:

- For Outlook users reading IU Exchange email, please follow the instructions at Email Encryption and Signing with Outlook.
- For Thunderbird users reading IU Exchange email, please follow the instructions at Sensitive Data Policies and Email Encryption.
- For all others, please see the information at Sensitive Data Policies and Email Encryption and let us know if you need further assistance.

Secure Your Mobile Devices

Please see the KB page Mobile Device Security Standards for information about securing your mobile devices (phones, tablets, laptops) so you are in compliance with IU security policies.
SSH Key Security

If you use OpenSSH keys (common in the Linux environment) you should follow these guidelines:

- Use key passphrases that meet the IU Passphrase Guidelines.
- Limit the scope of access for any keys you add to your authorized_keys file as much as possible. For example, you can proceed the key with `from=*.indiana.edu,*.iu.edu` to limit access to systems in those 2 domains. You can also use the `command=` directive to limit to a specific command.
- You are encouraged to avoid using password-less keys at all cost. When you create your keypair, you can create a password-less key by just hitting enter at the passphrase prompt. This allows anyone who gets your private key to have access without the need for a passphrase. Granted, there are some very limited cases where this is needed for unattended ssh operations (eg. via cron) but in such cases you must use the `from=` or `command=` directives to limit the scope of this key.
- Protect your private key as you would a password. You will likely have your public key in various locations and authorized_keys files, but limit the distribution of your private key file as much as possible. The private key should only be needed on the local system you are coming from and not remote systems you are logging into.

Understand Sensitive Institutional Data and Manage It Properly

One of the most important things you can do within the IU computing environment is understand what is, and isn't, sensitive institutional data and manage it properly. Sensitive data is classified as detailed in the Classifications of Institutional Data document. The classifications range from public information (eg. Names) to critical data (eg. Social Security Numbers, Health Information, etc). Here are some good starting points for understanding this important issue:

- What is sensitive data, and how is it protected by law?
- Classifications of Institutional Data
- Which IU services are approved for storing ePHI or other types of sensitive institutional data?
- SoIC Storage Services and Sensitive Data