CREATING STRONG PASSWORDS

Kevin Mitnick Security Awareness Training

"It's important to keep malware (malicious software) off your computer so hackers cannot intercept your passwords. Even if your passwords are very strong and hard to guess, malware can still allow a hacker to get them."

–Kevin Mitnick

Kevin Mitnick's 10 Rules for Stronger Passwords

Always use strong passwords on the internet. A strong password is one that is hard for someone else to guess.

1. Don't tell your passwords to anyone, even tech support people who may ask you for them. *Nobody* should ask for your password, and you should never give your password to anyone.
2. Don't use simple dictionary words or pets' or people's names for your password. And avoid things like your zip code or key dates like a birthday or an anniversary.
3. Use passwords that are at least 12 characters long; however, those are still easy to crack if an attacker gets into your network. If you want to be super safe, use 20 characters. And don't write them down where they can be easily found.
4. It's actually easier and more secure to create a passphrase instead of a password. A passphrase is a few nonsense words like *$3 for the pirate hat* or *Betty was smoking tires and playing tuna fish*.
5. Use a different password for each website. And don't use simple patterns like *password1*, *password2*, *password3* for different sites—those are too easy to guess.
6. Change your passwords for sensitive websites, like online banking, every 60-90 days, and, like Rule 5, do not use easy-to-guess patterns when you change them.
7. If you think your password may have been compromised, change it immediately and check your other websites for any signs of misuse, starting with your online banking site!
8. Sometimes websites ask you to enter the answer for a security question that you can use if you forget your password. Make sure that your answer to that security question is just as hard to guess as your password. This answer should not be used anywhere else.
9. Use extra security features, such as stronger forms of authentication, everywhere you can. For example, a site may offer an option to use Google Authenticator, which is an app that generates a new six-digit number every minute as a "second password." That is a good security feature, so use it! Sites also sometimes offer to send you a code via a text message. To log in to your account, you need both your password and the code. That's less secure than the Google Authenticator app on your phone but better than nothing.
10. Use the password procedures that your organization requires you to use, and consider using a password manager at home. These products make it much easier to have strong, unique passwords on all of your accounts. There are also online password generators that create hard-to-guess passwords—for example, www.passwordsgenerator.net.

KnowBe4
Human error. Conquered.

Tips for Password Security

- ☐ Keep your passwords private—never share a password with anyone else.
- ☐ Do not write down your passwords.
- ☐ Use passwords of at least 12 characters or more (longer is better).
- ☐ Use a combination of uppercase letters, lowercase letters, numbers, and special characters (for example, !, @, &, %, +) in all passwords.
- ☐ Avoid using people's or pets' names or words found in the dictionary. It's also best to avoid using key dates (birthdays, anniversaries, etc.).
- ☐ Substituting look-alike characters for letters or numbers is no longer sufficient (for example, "Password" and "P@ssw0rd").
- ☐ A strong password should look like a series of random characters.
- ☐ On the web, if you think your password may have been compromised, change it at once and then check your website accounts for misuse. At work, change your password at once, and then call your company's IT security help desk.

Password Management Software Products

In the office, your organization may not be able to use these, but for the house, there are good password manager software products on the market today. Some are free; none are very expensive. Using one of these products, you can create truly random, very long, and unique passwords for each site, and because the software will remember them for you, you never have to worry about what your password is. Your password manager will store and encrypt the passwords for you and log you in automatically. You will have vastly improved security, with only one master password to remember.

How to Create a Strong, Complex Password

Here's a way to make a strong password that's very hard to crack:

Follow These Steps	Example
1. Think of a phrase or sentence with at least eight words. It should be something easy for you to remember but hard for someone who knows you to guess. It could be a line from a favorite poem, story, movie, song lyric, or quotation you like.	**I Want To Put A Dent In The Universe**
2. Remove all but the first letter of each word in your phrase.	**IWTPADITU**
3. Replace several of the uppercase letters with lowercase ones at random.	**iWtpADitU**
4. Now substitute a number for at least one of the letters. (Here we've changed the lowercase "i" to the numeral "1.")	**iWtpAD1tU**
5. Finally, use special characters ($, &, +, !, @) to replace a letter or two—preferably a letter that is repeated in the phrase. You can also add an extra character to the mix. (Here we've replaced the "t" with "+" and added an exclamation point at the end.)	**iW+pAD1tU!**

This guideline on creating strong passwords is just a small section of the Kevin Mitnick Security Awareness Training. For more information and to train all employees, please visit **www.KnowBe4.com**.

© 2017 KnowBe4, Inc. All rights reserved. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

Microsoft

Password-less protection

Reduce your risk exposure with password alternatives

Contents

03 /
Introduction
Passwords are no longer enough

05 /
Why eliminate passwords?
Moving away from passwords

08 /
Introduction to password replacement technology
What do we mean by password-less authentication?

09 /
Adopting a password-less strategy
10 Choosing the right technology
- 11 Windows Hello for Business
- 13 Microsoft Authenticator app
- 14 FIDO2 security keys
- 16 Comparing the Microsoft technologies for password-less authentication

17 Understanding how strong authentication works
- 18 Secure authentication flow architecture
- 19 Common misconceptions

21 User adoption
- 22 Old-school mentality
- 22 Educating users on new authentication methods

23 /
Summary

Passwords are no longer enough

IT around the world see the beginning of a new era, where passwords are considered as a relic of the past. The costs now outweigh the benefits of using passwords, which increasingly become predictable and leave users vulnerable to theft. Even the strongest passwords are easily phishable. The motives to eliminate authentication systems using passwords are endlessly compelling and all too familiar to every enterprise IT organization. But how do you get there?

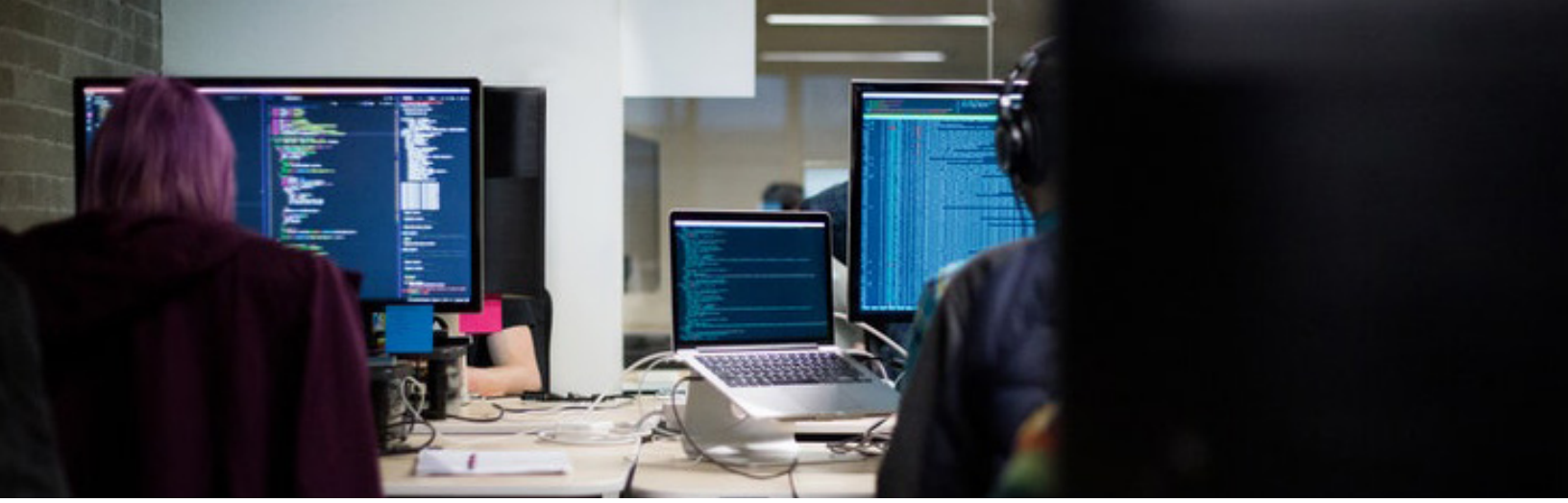
For enterprise IT departments, nothing costs more than password support and maintenance. It's common practice for IT to attempt lessening password risk by employing stronger password complexity and demanding more frequent password changes. However, these tactics drive up IT help desk costs while leading to poor user experiences related to password-reset requirements. Most importantly, this approach isn't enough for current cybersecurity threats and doesn't deliver on organizational information security needs.

81% of hacking-related breaches used either stolen or weak passwords

Source: Verizon 2017 Data Breach Investigations Report

You can reduce your odds of being compromised by up to 99.9% by implementing multi-factor authentication (MFA).

Source: Microsoft 2018 Security Research



Why eliminate passwords?

Password authentication has always been challenging throughout the evolving enterprise security landscape. A password is supposed to provide a key to accessing an account and a security barrier to protect the account from the attackers. To distinguish between the account owner and the attacker, organizations have needed to move beyond using just passwords for protection.

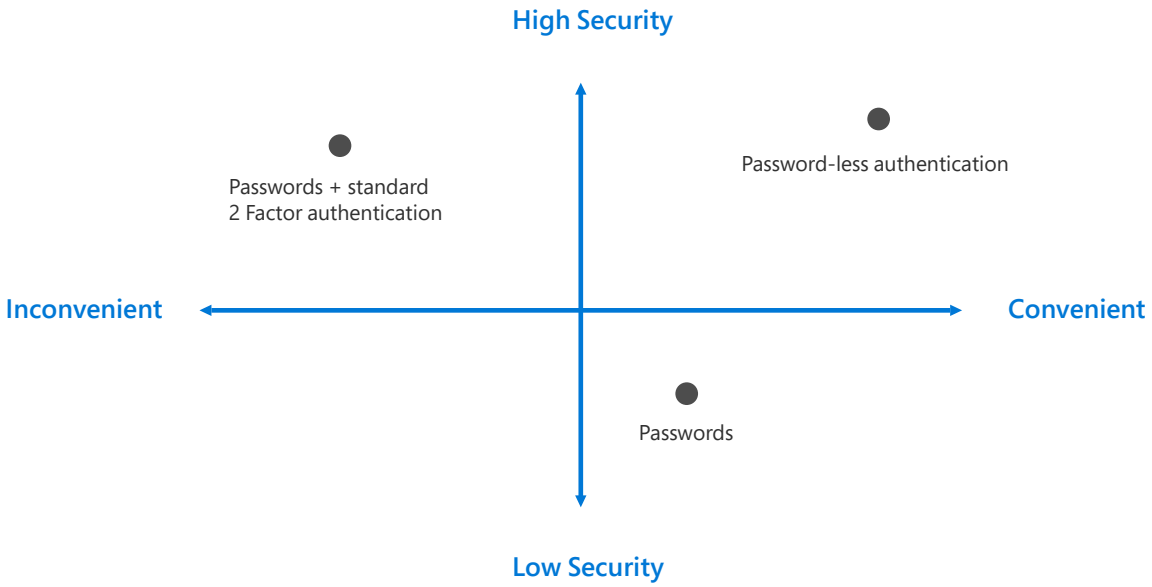
Multi-factor authentication (MFA)—for instance, a pin and password, or biometrics—has presented a more secure method for organizations. With increasingly complex access environments and more access points than ever before, IT teams have every reason to add multi-factor authentication options such as smart-cards, hard and soft tokens, SMS, and more—wherever users connect to resources. By going beyond passwords to add authentication steps, you can make user access to your resources more secure.

However, depending on the implementation, MFA can also lead to increasing complexity regarding the user experience. It's imperative for for IT teams to deliver a seamless user experience while balancing security risk.

Many years ago, we started multi-factor authentication with smart-cards to secure the identity of our employees. Initially, we used physical smart-cards to secure, but it didn't give people a smooth user experience. Additionally, this also requires a card reader in each hardware device which can be challenging to implement and also smart-cards are prone to be lost or forgotten. Then we focused on a nearly-friction-free experience, from using biometrics that allows people to use fingerprints, iris scans, facial recognition, and even heartbeats to authenticate their identity. These technologies are easier to use, more accessible to the needs and preferences of the person, and are significantly harder for criminals to exploit.

–Bret Arsenault, CVP & CISO, Microsoft

Source: Enterprise Security magazine



Today, IT security are moving toward password-less authentication using advanced technologies like biometrics, PIN, and public/private key cryptography. Plus, new standards like Web Authentication API (WebAuthN) and Fast Identity Online (FIDO2) are enabling password-less authentication across platforms. These standards are designed to replace passwords with biometrics and devices that people in your organization already use, such as security keys, smartphones, fingerprint scanners, or webcams.

Password replacement options can help organizations provide convenience and ease-of-use without high-security risks. Ideally, with password-less authentication, you can have a future ecosystem of authentication that meets the organizational needs of high security and privacy, usability, and interoperability among different authentication devices.

Moving forward, end-users should never have to deal with passwords in their day-to-day lives. And with an intuitive sign-in/sign-up user experience, help desk costs can be reduced.

Introduction to password replacement technology

What do we mean by password-less authentication?

Password-less authentication, as we refer to it in this brief, is a form of multi-factor authentication that replaces the password with a secure alternative. This type of authentication requires two or more verification factors to sign in that are secured with a cryptographic key pair. The device creates a public and private key when registered. The private key can only be unlocked using a local gesture such as a biometric or PIN. Users have the option to either sign in directly via biometric recognition—such as fingerprint scan, facial recognition, or iris scan—or with a PIN that's locked and secured on the device.

Adopting a password-less strategy

At its core, the underlying principle of password-less authentication is to eradicate the use of passwords and thereby drain their value for attackers. Moving forward with this approach requires technologies that can support it—and time for organizations and users to adopt these technologies. Adoption also involves a new mindset. Organizations have to understand how the approach works with their flow of operations and make the necessary technical and cultural shift, so that users can operate in this new password-less world.

Here are the key considerations for implementing password-less authentication into your MFA strategy:

1. Choosing the right technology – Develop password-replacement offerings with a new set of alternatives that address the shortcomings of passwords while embracing their positive attributes. This early stage is about implementing an alternative and getting users acquainted with it.

2. Understanding how it works – Get to know how password-less technologies overcome security challenges and reduce the user-visible password-surface area. Adopting these technologies means upgrading experiences related to the life-cycle of a user's identity—including provisioning of an account, setting up a brand-new device, using the account/device to access apps and websites, and enacting recovery. It also means deconditioning users from providing a password any time a password prompt shows on their computer.

3. Increasing user adoption – Simulate a password-less world—that is, enable end users and IT admins to replicate the approach in a test environment and transition into a password-less world with confidence. This simulation should encourage a cultural shift within the organization—getting users comfortable with the idea of never typing, changing, or even knowing a password going forward.

Choosing the right technology

With biometrics on mobile phones and computers becoming more ubiquitous, the number of password replacement technologies has increased.

Microsoft offers solutions based on platform, hardware, or software that you can try out today and map with your password-less authentication requirements. Introduced by Microsoft in Windows 10, Windows Hello uses biometric sensors or a PIN to verify a user's identity. The Microsoft Authenticator app is a software token that allows users to verify their identity with a built-in biometric or a PIN when signing into their work or personal accounts from a mobile phone.

As a member of the FIDO Alliance, Microsoft has been working with other alliance members to develop open standards for the next generation of credentials. As a result, you can now use portable FIDO2 hardware devices to log into a work machine or cloud services on supported devices and browsers.

Let's go into more detail on each of these technology options.

Windows Hello for Business

Windows Hello for Business replaces passwords with strong multi-factor authentication on Windows 10 platforms, including PCs and mobile devices. This authentication consists of a new type of user credential that's linked to a device and uses a biometric or PIN. It lets you sign in with your face, iris scan, fingerprint, or a PIN, and enables you to authenticate to enterprise applications, content, and resources without a password being stored on your device or in a network at all. The biometric data is only used locally and never leaves the device.

How it works

The Windows Hello provisioning process generates a cryptographic key pair bound to the Trusted Platform Module (TPM) on a device. Access to these keys and obtaining a signature to validate user ownership of the private key is enabled only by the PIN or biometric gesture. Taking place during Windows Hello enrollment, the two-step verification creates a trusted relationship between the identity provider and the user. When a user makes the gesture through the device, the provider is able to verify the identity from the combination of Hello keys and the gesture. This activates an authentication token that allows Windows 10 to access resources and services. For further information, go to Windows Hello for Business and Authentication.

Windows Hello for Business is personal, simple, and provides a brilliant user experience with high security. Our people love logging on with their fingerprint or face.

–Peter Scott, Director of Dynamic IT, British Telecom Technology

As of October 2018 there are 89 million active Windows Hello users worldwide. More than 6,500 organizations have deployed Windows Hello for Business. Major PC vendors are shipping devices that have integrated Windows Hello-compatible cameras or fingerprint readers.

Microsoft Authenticator app

Millions of people are using the Microsoft Authenticator app every day to better secure their sign-ins.

The Microsoft Authenticator app enables users to verify their identity and authenticate to their work or personal account. Microsoft Authenticator can be used to augment a password with a one-time passcode or push notification. The app can also be used to verify multiple factors and replace the need for a password. Instead of using a password, users confirm their identity using your mobile phone through fingerprint scan, facial or iris recognition, or PIN. Built on secure technology similar to what Windows Hello uses, this tool is packaged into a simple app on a mobile device making it a convenient option for users. The Microsoft Authenticator app is available for Android and iOS.

How it works

In place of encountering a password prompt after entering a username, users get a push notification to verify presence. In the app, users confirm their presence by matching a number on the sign-in screen, then providing a face scan, fingerprint, or PIN to unlock the private key and complete the authentication. This multi-factor verification method is more secure than a password and more convenient then entering a password and a code. In some cases it doesn't require any typing at all! For further information, go to How to use the Microsoft Authenticator app.

FIDO2 security keys

FIDO2 is an evolution of the U2F open authentication standard based on public key cryptography using hardware devices. This standard is intended to solve multiple user scenarios including strong first factor (password-less) and multi-factor authentication. With these new capabilities, a security key can entirely replace weak static username/password credentials with strong hardware-backed public/private-key credentials. These credentials cannot be reused, replayed, or shared across services. Devices and tokens that adhere to FIDO2, WebAuthN, and CTAP protocols bring about a cross-platform solution of strong authentication without using passwords. Microsoft partners are working on a variety of security key form factors, such as USB security keys and NFC-enabled smart cards.

How it works

Microsoft has been working with partners to ensure FIDO2 security devices work on Windows, the Microsoft Edge browser, and online Microsoft accounts, to enabling strong password-less authentication. For shared device scenarios, security keys allow you to carry your credential with you and safely authenticate to an Azure AD joined Windows 10 device that's part of your organization. You can use any shared Windows device belonging to your organization and authenticate securely—without needing to enter a username and password or set up Windows Hello beforehand. Unlike traditional passwords, these keys rely on high-security, public-key cryptography to provide strong authentication. Plus, these keys have all the benefits of a secured enclave to store credentials while also being portable, enabling more use cases for deskless and kiosk workers.

Security devices fit nicely with our current scenarios. They are simple to deploy and easy to use. We see value in rolling FIDO2-enabled HID badges to all 110,000+ Emirates Group staff in the future.

–Emirates IT

Microsoft has been aligned with the FIDO Alliance from the start; the alliance represents 250 organizations from various industries on a joint mission to replace passwords with an easy-to-use, strong credential.

Comparing the Microsoft technologies for password-less authentication

Here are some factors for you to consider when choosing Microsoft password-less technology:

	Windows Hello for Business	**Microsoft Authenticator app**	**Fast Identity Online (FIDO) 2 security devices**
Pre-Requisite	Windows 10, version 1511 or later Azure Active Directory	Microsoft Authenticator app Phone (iOS and Android devices running Android 6.0 or above.)	Windows 10, version 1809 or later Azure Active Directory
Mode	Platform	Software	Hardware
Systems and devices	PC with a built-in Trusted Platform Module (TPM) PIN and biometrics recognition	PIN and biometrics recognition on phone	FIDO2 security devices that are Microsoft compatible
User experience	Sign in using a PIN or biometric recognition (facial, iris, or fingerprint) with Windows devices. Windows Hello authentication is tied to the device; the user needs both the device and a sign-in component such as a PIN or biometric factor to access corporate resources.	Sign in using a mobile phone with fingerprint scan, facial or iris recognition, or PIN. Users sign in to work or personal account from their PC or mobile phone.	Sign in using FIDO2 security device (biometrics, PIN, and NFC). User can access device based on organization controls and authenticate based on PIN, biometrics using devices such as USB security keys and NFC-enabled smartcards, keys, or wearables.
Enabled scenarios	Password-less experience with Windows device. Applicable for dedicated work PC with ability for single sign-on to device and applications.	Password-less anywhere solution using mobile phone. Applicable for accessing work or personal applications on the web from any device.	Password-less experience for workers using biometrics, PIN, and NFC. Applicable for shared PCs and where a mobile phone is not a viable option (such as for help desk personnel, public kiosk, or hospital team).

Understanding how strong authentication works

Secure authentication flow architecture

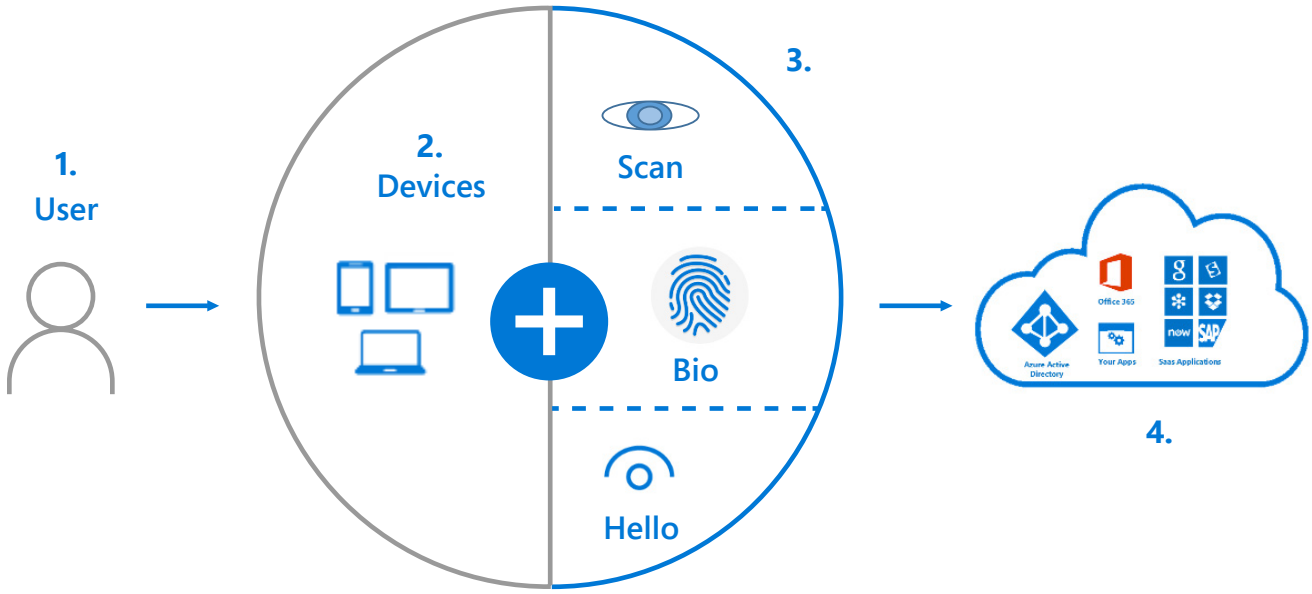
All three technologies use the same proven cryptographic authentication pattern, with credentials based on the certificate or asymmetrical key pair. These credentials—plus the token that is obtained using the credential—are bound to the device (Windows or FIDO2 device, or mobile phone).

The authenticator generates a key pair and returns the public key. Optionally, the authenticator also returns an attestation to the identity provider such as Azure Active Directory.

Identity provider validates user identity and maps the public key to a user account during the registration or provisioning step. Authentication requires multiple factors, combining a key or certificate tied to a device and something that the person knows (a PIN) or something that the person is (biometrics). Private keys are securely stored on the device. Private keys are bound to a single device and never shared. These keys don't roam and are never sent to external devices or servers.

This kind of authentication requires a local gesture. PIN entry and biometric gesture both trigger devices to use the private key to sign data that's sent to the identity provider cryptographically. The identity provider verifies the user's identity and authenticates the user.

Secure authentication flow architecture



1. The user attempts to sign into their account from a device. The device sends an authentication request. The identity system (for example, Azure AD) requests validation.

2. The user interacts with a local gesture (for example, biometric, PIN) from its device. The device uses the private key to sign nonce and returns to Azure AD with key ID. A request/signature containing both the nonce + the key ID signed with the device key sent to Azure AD

3. Azure AD verifies the signature with the public key in the user object and verifies nonce. Builds a Primary Refresh Token (SSO token) and an ID token and send them back along with an encrypted session key. The user accesses applications without the need of authenticating again (SSO).

Common misconceptions

Misconception 1:

Isn't a PIN the same as a password?

A PIN looks much like a password, which may lead people to equate them. A PIN can be a set of numbers, but enterprise policy might allow complex PINs that include special characters and letters, both uppercase and lowercase. However, it's not the structure of the PIN that makes it better (length, complexity), but rather how it works. A PIN is tied to the specific hardware device it was set up on. Without the device, the PIN is useless. If someone stole your PIN and wanted to sign in to your account, they'd need your physical device too.

Misconception 2:

If I use password-less authentication, doesn't that impact my legacy app and protocols?

Adopting password-less authentication when still using legacy protocols does present challenges. However, for this purpose, Microsoft is developing a time-limited password—a kind of one-time password with a current time or a time limit that the user could generate when using legacy authorization.

Misconception 3:

Can't a biometric access system get hacked or spoofed?

Microsoft understands how critical it is to protect your biometric data from theft. For this reason, your "biometric signature" is secured locally on the device and shared with no one but you. Plus, your signature is only used to unlock your device and never to authenticate you over the network. As it just stores biometric or PIN identification data on the device, there's no single collection point an attacker can compromise to steal biometric data.

In a typical deployment of the FIDO2 and Windows Hello, a user swipes a finger, speaks a phrase, or looks at a camera on a device to sign in. Behind the scenes on that device, the biometric is used as an initial factor to then unlock a second, more secure factor: a private cryptographic key that works to authenticate a user to the service.

A common biometric attack method involves trying to spoof a person's body part, with the goal of tricking the system into thinking that a fake is real. Any spoofing or hacking attack would first require that the attacker gains custody of the device. Beyond the various layers of protection, many biometric systems today are building in "liveness detection" to validate that a biometric presented is real.

User adoption

No change is easy. Cultural and technical challenges follow organizations as they proceed with password-less authentication methods.

Every organization is complex; while password-less authentication offers improved security and user experience, most organizations need to fix many fundamental facets to start on this journey. These fixes can be implemented over time to additional groups to reduce your risk of attacks and security breaches. That effort offers rewards, however. From a technological viewpoint, reducing the use of passwords and eventually eliminating them can help you make a sea change in both security and productivity for your organization.

Getting rid of passwords can help you enjoy these benefits:

As a user, you can sign in faster to use applications and services. There are no passwords to create, store, or remember.

Password-less authentication delivers a higher degree of trust and security for apps, devices, and service providers. You don't have to store passwords.

It's cost-effective for IT. IT support teams can be freed from endless password problems.

Old-school mentality

It's nearly impossible for an organization to visualize how different individuals go about their day-to-day activities, or to validate this password-less change accurately. It's crucial for organizations to do just that. Understand that you're encouraging people, including many in IT leadership, to switch from a widely adopted security system, like passwords, that's very familiar, comfortable, and conventional. And don't forget: change for most people is hard. Yet, in this case, once users experience password replacements, they'll forget that they even needed to enter passwords on a day-to-day basis or reset passwords on their own in a self-service portal. You need to make them realize it's simpler, better, and help them erase the mentality that a password is the key to their world. Passwords are not enough anymore. It's time to go to the next level of authentication.

Educating users on new authentication methods

The successful evolution of password-less authentication heavily relies on user acceptance. An awareness drive on these new password-less authentication methods can help users understand and affirm the new way of authenticating to their devices, such as using Windows Hello for Business or Microsoft Authenticator-based applications.

Organizations need to educate their users that:

1. Hackers easily guess passwords. One encouragement could be that MFA is simply making their password authentication better and stronger.

2. Companies that have experienced data breaches may have leaked user data to the web. Hackers that obtain user information can use that information to guess further passwords because users often use the same, or a derivative password, for several sites or services.

3. Phishing efforts often lead users to sign in to fake sites, giving their usernames and passwords away. With password-less authentication, this is an issue of the past because the physical keys are bound to the machines they use and FIDO2 tokens will not authenticate with a website it doesn't trust.

This awareness practice can answer some of the objections, encourage questions and feedback, and explain the value of this change. The user education enables and inspires users to try the experience out.

Summary

The adoption of modern multi-factor authentication technologies—like biometrics and public key cryptography in widely accessible devices—is one of the most impactful steps that can meaningfully reduce a company's identity risk. Given emerging requirements, organizations can prepare themselves by making a plan to start moving to to password-less technologies.

Going password-less is a long-term approach for secure authentication, and it's still evolving. It can take time to transition. You can start with a pilot of one or more options. For users that can't go password-less, turn on MFA to validate users and minimize prompts based on the risk of the sign-in with conditional access capabilities. Use a password filter to block leaked credentials and common passwords from being used with password protection policies.

For more information, here are some resources that can help you get started:

Overview of Microsoft password-less technologies

Windows Hello for Business documentation

About the Microsoft Authenticator app

© 2018 Microsoft Corporation. All rights reserved. This document is for informational purposes only. Microsoft makes no warranties, express or implied, with respect to the information presented here.

HOW CRIMINALS COMMIT ID THEFT

ID thieves are always looking for ways to steal your personal information. Here are some examples:

Mail Theft

By stealing your mail, thieves can get your personal information from bills, statements, etc.

Dumpster Diving

Thieves can go through your garbage to find old bills and recent receipts.

Data Breaches

Companies you do business with could be storing your personal information. If there's a breach, your info could be compromised.

ATM Overlays

These are devices thieves install at ATM machines and gas pumps to steal your account information when your card is swiped.

Change of Address

Thieves can change your address to steal your mail to commit identity theft.

Malware & Viruses

Your computer can be hacked through websites, Internet programs or file-sharing networks allowing thieves to access your private personal information.

Stolen Wallet

While some thieves might be after money, others are more interested in your personal identification to steal more than just cash.

Shoulder Surfing

Thieves stand behind you and watch as you enter passwords, personal identification numbers or private information.

Keystroke Logging

On public computers, gas pump displays and ATM keypads, criminals can install technologies to record the buttons you press as you enter card numbers or passwords.

Vishing

Phone scams that request personal information either by a direct caller or through voice messages.

Online Shopping

If you mistakenly shop at a fictitious retail website or through unsecured payment systems, your credit and debit cards could be at risk.

The Dark Web

This is an underground, online community where criminals can go to buy and sell your personal information.

Phishing

These are fake emails that can look surprisingly legitimate. If you get tricked into clicking a link or providing information, thieves can get your passwords and account numbers.

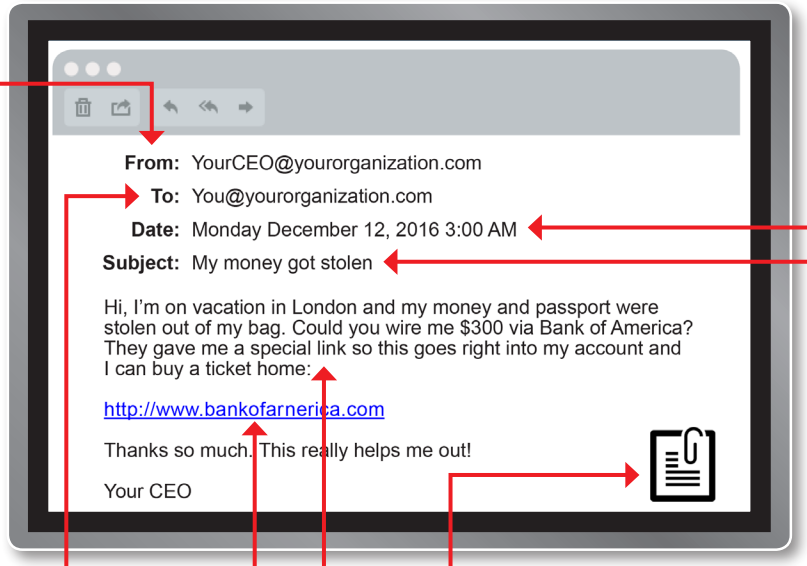
Smishing

Phishing through a Short Message Service (SMS) or text message. The message will direct you to visit a website or call a phone number.

Social Engineering Red Flags

FROM

- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.



DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

© 2017 KnowBe4, LLC. All rights reserved. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

Idaho State University's Geospatial Coordinating Committee

Best Practice Guidelines for Data Retention and Deletion

Management of digital geospatial data has special requirements as indicated by the *Idaho State Board of Education Records Management Guide* (section 4, special requirements). This document sets forth a policy for the retention and deletion of digital geospatial data for research projects of the ISU GIS Training and Research Center. The policy presented here also serves as a recommendation to the broader ISU geospatial community on best practices for the management of digital geospatial data associated with sponsored research. These best practices conform to the Idaho State Board of Education (SBOE) guidelines as well as American National Standards Institute (ANSI) and International Organization for Standardization (ISO) standards.

Terminology used in this document

- *Active geospatial dataset*: A geographic information system (GIS) or remote sensing (RS) file or collection of files used in normal business activities. These files are typically research or framework data sets stored in a standard geospatial data format. Global positioning system rover files (field data collected by researchers using GPS receivers) in raw or corrected formats are not considered active geospatial data sets until they are converted into a standard geospatial data format. Global positioning system base station files for the current calendar year are considered active geospatial data sets and follow the retention and deletion schedule described below.
- *Archiving*: the process of creating a duplicate copy of an electronic record for future reference. The permanent duplicate copy is stored off-site on a stable external media.
- *Georeference requirements*: Each geospatial dataset should be projected and defined following the appropriate regional standard georeference system. For example, geospatial data for the state of Idaho, in accordance with the Idaho Geospatial Office standard for georeferencing, shall be properly projected and defined in Idaho Transverse Mercator. Data quality (i.e., horizontal positional accuracy) is not addressed by this policy.
- *Geospatial data set*: A GIS or RS file or collection of files.
- *Inactive geo-spatial dataset*: A GIS or RS file or collection of files that is no longer used in normal business activities. These files typically represent a collection of files generated during research that are intermediary to a completed product. These datasets should be stored in a *standard geospatial data format* (see below). In addition, global positioning system base station files for the previous calendar year are considered inactive geospatial data sets and follow the retention and deletion schedule described below.
- *Original data source*: A GIS or RS file or set of files stored in a data format that may or may not comply with the standard geospatial data format guideline. These files represent the status of the data as received. These data typically require various degrees of preliminary processing before they are ready for use in a GIS. Examples include non-georegistered and uncorrected satellite imagery.
- *Standard geospatial data format*: Vector data should be stored as shape files (*.SHP and all associated files that constitute a shapefile dataset). Raster data should be stored in an uncompressed format to include, but not limited, to ERDAS Imagine (*.IMG), ESRI floating point (*.FLT), or tagged image file format (*.TIF),

Data Retention Determination for Archiving
Geospatial data is an asset that should be treated and managed similar to cash or capital equipment. Apart from financial value, it is critical that geospatial data be managed properly to avoid loss due to versioning, corruption, or deletion. Additionally, geospatial data must be managed as a historical dataset for temporal change detection analyses and other purposes. Each Principal Investigator, with guidance from the GIS Director, is responsible for managing geospatial data over the life cycle of that specific data set (generation or acquisition through inactive geospatial data archiving).

Not all geospatial data produced at Idaho State University will be permanently archived. Due to the fact that geospatial data sets are large (many datasets exceed 1GB) it is important to recognize that permanently archiving all geospatial data (i.e., all versions, iterations, and preliminary processing data sets) is not feasible. Instead, geospatial data will be permanently archived to preserve:

- The original digital data source.
- Original digital data that has been processed into a standard geospatial data format.
- Final geospatial datasets stored in a standard geospatial data format, with proper georeferencing, and metadata documentation. These data represent the completion of a model, deliverable, or data layer. All metadata shall follow the Federal Geographic Data Committee (FGDC) standard for geospatial metadata documentation.

Data Deletion Schedule
Upon completion/expiration of a grant or contract, all geospatial data produced during the life of the project should be examined by the principal investigator. Geospatial data should be inventoried and sorted into one of two general categories (retain or delete). If a geospatial dataset satisfies the retention determination described above, that data must be retained for permanent archiving. If it does not satisfy the criteria, deletion of the geospatial dataset is at the discretion of the investigator. If the principal investigator is unsure of the correct status for a geospatial data set, he/she should contact ISU's GIS Director for clarification.

Data Storage Guidelines
<u>Preliminary backup</u>
Initially all geospatial data satisfying the criteria set forth above will be copied to the GIS TreC's spatial library server or other server meeting the following hardware requirements:

- Hardware RAID 5 fault tolerance
- All hard drives must be hot-swappable
- Dual redundant power supplies

These hardware requirements are critical to insure safe and secure storage of geospatial data sets to aid in the prevention of loss due to corruption.

<u>Permanent Archive</u>
All geospatial data meeting the criteria set forth above for permanent archiving will be stored on the GIS TReC's off-site server or other off-site server meeting the following requirements.

- Hardware RAID 5 fault tolerance
- All hard drives must be hot-swappable
- Dual redundant power supplies

Alternatively, external solid state drives may be used and should also be stored off-site once data has been copied and verified on the drive.

A viable off-site location is an important consideration and should be a site that is owned/maintained by Idaho State University and physically disconnected from the source of the original data (e.g., the GIS TReC in Graveley Hall). Ideally, this location will be climate controlled and located above grade to minimize potential flooding disasters.

A permanent archive of geospatial data stored in preliminary backup will be created at intervals not to exceed 60 days. Data should not be bundled or compressed (e.g., ZIP or TAR compression) and the media used will conform to industry standard media types. Important considerations regarding archive media are:

- Sensitivity of media: Will problems be encountered due to media sensitivity to heat, humidity, and light? This consideration is perhaps most important even though archive media should be stored in an environmentally controlled facility.
- Assurance of media: Is the data stored on the media in a format that will be readable in the future? This consideration is of secondary importance as long as the selected media conforms to current ISO and/or ANSI standards. Most available media meets this criterion.
- Longevity of media: How long will the media be viable? This concern is perhaps least important, relative to those listed above.

The GsCC recommends the use of live, real-time server based archiving solutions employing a hardware RAID 5 fault tolerance solution with adequate power monitoring and uninterruptable power supply (UPS) to allow for a safe system shutdown in the event of prolonged power outage . The above server should be physically secured and use strong authentication to better ensure the integrity and security of the archived data. In accordance with guidelines set forth by the American Society of Heating, Refrigerating, and Air-Conditioning Engineers (ASHRAE) the physical environment within which the server operates should be maintained with ambient air temperature between 20° C (68° F) and 25° C (77° F) and relative humidity levels between 40-55% (ASHRAE TC9.9).

In the event that archived data need be retrieved, the retrieval process shall be completed within 3-business days of receipt of the retrieval request by ISU's GIS Director.

Contingency and Data Assurance

It is the responsibility of the GIS TReC administration to periodically assess the viability of archived data by retrieving a randomly selected media and ensuring it is readable and functional by at least one current version of a GIS/RS software application. Should it be determined that an archive has failed, all archive data will be retrieved, tested, and all recoverable data transferred to new media. To eliminate or reduce this problem, data will be cycled to new media following the schedule given below:

- All geo-spatial data stored on archive quality CD or DVD will be read and duplicated to a new archive quality CD or DVD every 10 years or as deemed necessary by the GIS Director. Re-examination schedule will be clearly marked on each CD or DVD.

Should it be determined that a standard geospatial data format has become obsolete, all data stored in that format will be re-processed using legacy software and converted to a new and compliant format.

These guidelines shall be reviewed and revised by the GsCC as necessary with a review interval not to exceed five (5) years.

The following excerpt has been taken from the *Idaho State Board of Education Records Management Guide* (section 4).

Part I. **Electronic records (E-Records)**

1. *Requirements for E-Records.* Records generated and stored on computers and related systems must be monitored and assessed for value in relation to the SBoE and the Institution's record retention schedules. These records shall be inventoried just as if on paper, and have destruction or preservation timeframes established as with other record formats. Present Idaho code refers to ANSI standards for digitized paper or photographic files as the benchmark for recordkeeping. However, new standards are in review which address a broader and more flexible set of criteria for the management of electronic records. These are standards for the content of *information identifying the type and format of data in an electronic file*, or the *metadata*, so that across time these files will potentially remain more accessible regardless of platform and application software.

2. *Principles of E-Records Management.* The following principles of electronic records management should be adhered to in both operation and planning of the work of higher education institutions:

    - Computers and computer backups should be organized with attention to the life expectancy (retention) of the information being created and stored;
    - Institutions are encouraged to migrate on a periodic schedule to newer platforms, media, and systems those records designated Permanent according to the SBoE Records Retention Schedules, with authentication and quality assurance checks to ensure data and file integrity after transfer;

3. *SBoE Guide, State and Federal Requirements.* E-Records created in the normal course of official business and retained as evidence of official policies, actions, decisions or transactions are records subject to the management requirements of this Guide. Specific legislation may also affect retention requirements e.g. Federal Limitations Act (disabilities law), state Rules of Evidence, Uniform Code of Evidence (applicable in many states) and the Federal Income Tax Act, etc.
    - Records communicated in an electronic format need to be identified, managed, protected, and retained as long as they are needed to meet operational, legal, audit, research or other requirements.
    - Records needed to support program functions should be retained, managed, and accessible in existing filing systems outside the e-mail system in accordance with the appropriate departments standard practices.
    - Originators of e-records within the Institution are responsible for proper filing and retention of those e-records. Additionally initial (original) recipients of e-record from institutions and individuals outside the Institution are similarly responsible for filing such records.
    - *Disaster Recovery.* Information Technology administrators and internal control (and/or internal audit) staff are responsible for maintaining electronic record security, backup, and for disaster recovery plans for those records placed under their administration.

Idaho State University's
GIS Training and Research Center
Data Sharing Policy

1. Executive summary

The GIS Training and Research Center's (GIS TReC) project activities involve the development of spatial and non-spatial databases on bio-physical and natural resource features within various project areas. Ensuring proper access to these data by project partners, collaborators and the general public is important for carrying out the mission of the GIS TReC. Therefore, a clear data sharing policy, facilitating access to data and their responsible use is necessary. This document provides policy guidelines for sharing different types of data acquired or generated by the GIS TReC along with the responsibilities of the custodians and end-users of these data, and serves as a guideline for proper documentation of data by GIS TReC personnel.

2. Introduction

The mission of Idaho State University's GIS Training and Research Center (GIS TReC) is to facilitate sound decision making through the use and application of geospatial technologies. While it is appreciated that results derived from geospatial analysis must not be applied as a comprehensive decision *making* tool, it is similarly recognized that these same results, and the data produced throughout the research/analysis process, are critical decision *support* tools. Consequently, a requisite for achieving the mission of the GIS TReC is data sharing.

3. Purpose of the data sharing policy

Data is widely recognized as a critical, essential, and valuable resource. The full potential of this resource can only be realized if it is discoverable, accessible and used appropriately by those who require it. Today, many projects involve a number of partners, national collaborators, national and international researchers who are all engaged in the collection and development of primary and secondary data within different thematic areas of a given study. Sharing and integration of these data is important to avoid duplication and wasted resources. This document outlines the policy adopted by the GIS TReC to facilitate data sharing within and outside project partners and the general public, as well as the responsibilities and rights of data custodians and end-users users.

4. Data types

As a result of the rangeland research efforts completed at the GIS TReC, various electronic data have been collected including various data types that may need specific management.

4.1 Vector spatial data

Spatial data includes data describing geographic and thematic layers (e.g., hydrography, land cover, and administrative boundaries) for use within a geographic information system (GIS). These data are usually large in quantity and need specialized software for viewing and manipulation.

4.2 Raster images

Remote sensing images from different satellite systems are frequently used for project activities and shared among the project partners and stakeholders. Similarly, other raster images (e.g., digital elevation models) are commonly used and shared. These data are usually large in size and like vector spatial data, require specialized software for viewing and manipulation.

4.3 Non-Spatial data

Data providing descriptions of spatial or aspatial features such as demography, research protocols, etc. and stored as non-spatial data in the form of tables. With the appropriate development of relationship classes these data may be linked as attributes of spatial data.

4.4 Documents

Other types of data associated with projects are in the form of documents such as manuscripts, publications, presentations, and posters which may be of interest to stakeholders as well as the general public.

4.5 Models

The GIS TReC has developed qualitative and quantitative models which will be of interest to scientists, researchers, and managers. Such models will be available as UML model diagrams or graphic file representations of the model.

4.6 Multimedia products

Multimedia products include videography, photography, and video files which may be of interest to stakeholders and the general public.

5. Data Categories

Depending upon the data sources and additional processing requirements, each data file, dataset, or database can be classified into the following categories.

5.1 Raw data

Throughout its research processes, the GIS TReC has collected large amounts of data through various sampling campaigns and measurement/monitoring activities. These data, as collected or acquired, require processing and analysis before being usable or meaningful in the context of the project. Once processed, they have the status of Primary source data

5.2 Primary source data

The data generated by each research project through field data collection or other methods are referred to as the primary source data once these data have been entered into an appropriate geodatabase structure with derivative calculations, relationship linkages, and geospatial metadata documentation.

5.3 Secondary data

In many cases, the data are compiled from existing sources which are in public domain or are acquired for the project through arrangements with other entities.

5.4 Value added products

These are data which are derived through processing and analysis of primary and secondary data. The processing involves value addition in terms of the information and knowledge generated from the underlying data set. For example, the development of NDVI and cNDVI raster data is produced through atmospheric correction and application of a simple band ratio to Landsat primary source data.

6. Metadata

Metadata is effectively data about data. It facilitates data sharing and use by providing information on the content, quality, and accessibility of each discrete data file or geodatabase. In turn, metadata provides the medium for data discovery by stakeholders, collaborators, and the general public. Different templates of metadata may be used for specific data types, though metadata produced at the GIS TReC is based on ISO standards for spatial data.

7. Data Sharing Policy

7.1 Data custodianship

The principal investigator or project team leader shall be the *custodian* of the data generated by the project including its collaborators. The *custodian* will be responsible to:

- Identify appropriate data category for each dataset (cf. section five above).
- Provide a metadata document for each applicable dataset in a format consistent with project specifications.
- Identify and document access rights to the data within the metadata.
- Ensure appropriate access restrictions have been applied to each dataset using electronic and physical data security measures as warranted.
- Ensure appropriate processes to maintain data integrity have been implemented.
- Ensure applicable copyrights are adhered to as set by the data producers/ distributors (e.g., satellite images, data from secondary sources)
- Ensure the privacy of individuals and that reasonable security measures are in place to unauthorized access, modification, and disclosure of personal data.
- Follow the GIS TReC Data Retention and Deletion Policy for backup and archiving of data (http://giscenter.isu.edu/gscc/toPDF/Retention and Deletion of Data_v7.pdf)
- Should the *custodian* leave the institution prior to completion of the project, it is the responsibility of the *custodian* to designate a replacement *custodian* prior to his/her departure. If this is not done, the GIS Director shall have the authority to seek and appoint a replacement *custodian*.

7.2 Data repository

A central data repository for GIS TReC project data has been established at the GIS TReC with physical records also maintained at that location. Each *custodian* will provide metadata to the GIS Director in accordance with section 7.1 above. They will also provide the data which they wish to share with partners, stakeholder and/or the general public. Access rights and restrictions must be made clear in the metadata. The metadata will be served on-line through the GIS TReC website available at http://giscenter.isu.edu with data request/download options dependent upon access rights of each particular dataset.

7.3 Data access

Access is a fundamental issue in the exchange of data. Information is valuable when it is discoverable and becomes accessible to the user. While data access should initially be unrestricted, it may differ based on user type (project team members, collaborators outside the university, and the general public) relative to data licensing agreements of acquired raw data (e.g., satellite imagery purchased from SPOT image corporation), for example:

The data access policy for each data set will be indicated in the metadata. As a general rule, the following policy will be followed:

7.3.1 Data access guideline based on data type:

- Primary datasets produced by the project will be made available following the policy described in the following section (7.3.2).
- Copyright and regulated datasets will not be distributed outside the rules set forth in the copyright or redistribution license/agreement but will be maintained. If the GIS TReC is not authorized to redistribute the requested data, the requestor may be provided with source information.
- Value added products should be made freely available unless otherwise precluded by an outstanding restriction.

7.3.2 Data access guideline based on purpose of data use:

- *For use within the project activities*: Data will be freely available to project partners and collaborators for use within project activities unless restricted by its source. However, if the partner or collaborator wishes to use the dataset for activities not related to the project, the conditions for purpose of data use will be applied as described below.
- *For humanitarian activities*: Data will be made freely available to requestors who wish to use it for humanitarian purposes such as rescue operation or disaster relief. In case of copyright and regulated data, conditions specific to the dataset are applicable.
- *For all other activities*: Data will be made freely available to requestors who wish to use it for non-commercial purposes. In case of copyright and regulated data, conditions specific to the dataset are applicable. Users are obligated to acknowledge the project and data sources as described in the metadata.

7.4 Data usage

Users, by virtue of receiving data from the GIS TReC, have specific responsibilities as follows:

- Users are expected to report errors found in the datasets to the *custodian* from whom they obtained the data/information.
- Users shall comply with the copyright requirements described in the metadata.
- If a user updates the obtained data, these updates shall be sent back to the *custodian* at no cost to the *custodian*.
- Proper acknowledgement should be given to the project when results are based on use of the acquired data.
- Users must abide by the requirements of the Privacy Act[1] and other relevant statutes

7.5 Breach of conditions

The GIS TReC expects partners, collaborators, and users to abide with the terms and conditions under which the data were collected and/or transferred to them. In case of any breach of conditions, attempts will be made to resolve the dispute through dialogue. If not resolved, legal solutions may be sought depending upon the severity of the breach.

8. Future strategy

This data sharing policy has been prepared in view of the GIS TReC's operational management which can be amended. Data custodianship and repositories after the close of the project follow the Data Retention and Deletion Policy (http://giscenter.isu.edu/gscc/toPDF/Retention and Deletion of Data_v7.pdf)

.

[1] cf. http://www.justice.gov/opcl/privacyact1974.htm