Memorial Sloan Kettering Cancer Center

Information Security Handbook

Introduction to Information Security

The Information Security Office mission is to **PROTECT** our patients, workforce, and organization; and **ENABLE** MSK to achieve its strategic objectives by developing and managing a comprehensive, predictive, and innovative information security program.

Protect

To ensure its continued success**,** MSK relies on **Individuals**, **Information**, and **Infrastructure**. MSK's Information Security policies and processes are designed to minimize and manage risk to these assets. Whether it be patients or staff, clinical information or research, MSK systems or those of our partners, the Information Security Office is here to help you define and manage the information security risk.

Enable

Whether you are working with new and innovative technology, collaborating with external partners, or developing new workflows, the Information Security Office is here to partner with you and help enable these key initiatives.

Feel free to contact the Information Security Office with any questions or concerns.

Information Security Office

CONTACT
e-Mail: InfoSec@mskcc.org
Voicemail: 646-227-2751

RESOURCES
Visit the Information Security Office website for more information.
https://mskcc.sharepoint.com/sites/pub-InfoSec

Purpose of this Handbook

This handbook is intended to introduce you to Information Security at MSK, serve as a general reference for important concepts, and address common questions and concerns.

Beyond the contents of this handbook, you should familiarize yourself with all Information Security Policies, found on the MSK Intranet at the following address:

https://mskcc.sharepoint.com/sites/pub-ITStandards/SitePages/technology-standards-policy.aspx

Q **Why does MSK have Information Security Policies and Standards?**

A MSK Policies and Standards are designed to establish a consistent baseline approach to risk management across the organization and communicate key information security requirements to the many MSK stakeholders that use our technologies and data.

Acceptable Use of MSK Resources

The Acceptable Use Policy (IT-3024) can be considered a 'Terms and Conditions' for your use of MSK Information Resources (data, technology, services, etc.). It defines the general requirements to which all workforce members must adhere to retain access.

Some important things to remember:

Work Resources are for Work Purposes. MSK resources are intended to be used to fulfill your job responsibilities and support MSK initiatives. Exercise good judgement and adhere to management direction with regards to any personal use.

MSK Monitors Network and System Activity. All network and system activity is monitored and logged on a routine basis to support security incident response processes and to ensure compliance with applicable laws and MSK policies and standards.

Keep Personal and Professional Accounts Separate. Personal accounts (e.g. email, cloud-storage, etc.) are not to be used for MSK business purposes or to send/receive MSK information. Similarly, do not use your MSK email to register for non-work-related services (utilities, banking, shopping sites, etc.). Not only does it put you at greater risk for phishing attacks, but should you terminate employment with MSK, you will immediately lose access to your MSK email account.

Guard Against Theft. All mobile electronic devices (e.g. Laptops, Phones, External Hard Drives, etc.) must be physically secured when left unattended; either with a cable lock, or within a locked cabinet, desk, or private office. All lost devices must be reported to the Help Desk immediately.

Do Not Circumvent Security. Any attempts to defeat MSK security controls may result in disconnection from the MSK network, management involvement, and corrective action. Installing or running any type of security tools (scanners, exploit toolkits, etc.) on or against MSK assets without the consent of the Information Security Office is strictly prohibited.

No Unsupported File Sharing Software. The use of peer-to-peer file sharing software on MSK computers or networks is strictly prohibited because it subjects MSK to malware infections and potential legal action. If there is a legitimate business need to share files outside of MSK, it must utilize one of the currently supported solutions.

Reporting Incidents: MSK's first line of defense is YOU.

An incident is any adverse event that is suspected or confirmed to cause harm to MSK data, Information Resources, or business processes. Examples of Information Security Incidents include:

Phishing/Social Engineering: Any attempt via email, phone, or in person, to solicit sensitive information or trick them into compromising their computer.

Virus or Malware Infection: Signs of infection include strange pop-ups, noticeable performance issues, and out of place or missing files.

Unauthorized Access or Use of MSK Information Resources: Access to MSK systems by unauthorized individuals or MSK workforce members misusing MSK information resources in ways contrary to what's expected under acceptable use or other information security policies

Loss or Theft of MSK Information Resources: Including, but not limited to data, PC's, mobile devices, thumb drives, etc.)

Security Events Reported by External Parties: Any reports of security issues involving MSK or a third-party which processes or stores MSK data.

Violations of Policy: Any other activity contrary to MSK Information Security Policy.

How to Report a Suspected Incident

If you believe that you have detected suspicious computer activity, or been the target of a cyber incident, it is imperative that you report it immediately. You can do so by either of the following methods:

- e-Mail the Information Security Office at infosec@mskcc.org
- Leave a message on the Information Security Office Voicemail at 646-227-2751
- If you need to speak with someone after-hours, you can call the Help Desk at 646-227-3337

KEY POLICY
IT-3035 Incident Response Policy

Q **What is the difference between Phishing and Spam?**

A If an unsolicited email directs you to reveal information (login/password, bank account information, etc.) or act (click a link, open an attachment, etc.), it is Phishing. If it contains unwanted news or attempts to sell you something, it is Spam.

If you suspect you've received a Phishing message, forward the email to infosec@mskcc.org so we can investigate.

Spam (aka "Junk Mail") can be forwarded to spamlab@mskcc.org so the email team can add it to MSK's Spam filters

Dealing with Data

While performing your job, it's important that you not only know what data you are working with but how MSK classifies that data. Depending on the classification, it would dictate how it needs to be handled or shared.

MSK has **three** classifications for the information it collects and uses. These are:

- **Sensitive.** Information that is not meant for broad internal or external use.
- **Internal-Use Only.** Information that is meant for broad internal use, but not for distribution outside of MSK.
- **Public.** Information that has been declared public knowledge by the appropriate personnel or department and can be freely given to anyone without any possible damage to MSK.

When working with MSK Information, there are a few things to keep in mind:

Ensure Authorization. Access to MSK Information Resources must only be provided to authorized individuals who require it to perform their job function. Be cautious who you share resources with and ensure that it is only provided to appropriate individuals.

Be Careful with Email. By default, email is not encrypted. Use MSKSecure whenever emailing sensitive information and instruct any third parties to encrypt any sensitive email being sent to MSK.

Use Encryption. Proper encryption must be utilized for any sensitive information sent outside of MSK or otherwise traverses an insecure, open network.

Q **Is it true that I should only worry about Information Security when I'm working with patient information?**

A No. While protecting PHI is important, it is not the only information MSK considers Sensitive. Sensitive Information includes Financial, Strategic, Employee, or any other data whose broad disclosure could adversely impact MSK. Both Sensitive and Internal-Use Only Information have requirements regarding their access, handling, and safe-keeping. If it's worth collecting, it's worth protecting.

Accounts and Passwords: Keys to the Kingdom

Any account which you are provided is meant to identify and prove who you are. Passwords are intended to protect you and must be kept private.

Do Not Share. You are responsible for all activities that occur within your account. To avoid being associated with actions that you did not perform, do not allow others to use your account and do not share your passwords.

Know When to Change Passwords. In addition to mandatory changes each year, be sure to change your password if it was created for you or you otherwise suspect someone else might know it.

Do Not Write Down Passwords. Passwords should be committed to memory. Like the above, passwords should not be discoverable (e.g. posted to the computer monitor, kept in a document, etc.).

Construct Secure Passwords. Adding special and mixed-case characters will make your password stronger but remember, length is always the most important factor in password construction. When constructed of multiple words, a long passphrase will be harder for a malicious hacker to "crack". For example, AllYouNeedIsLove is a stronger password than @llUN33dIsLuv and is easier to remember and type. Of course, choosing a passphrase that isn't easily guessable is also key so if your social media profile status says: "Huge Beatles Fan" you should definitely choose something else!

Do Not Use MSK Passwords on Non-MSK Accounts. Maintaining different passwords will help prevent a breach of one account from resulting in a breach of the other.

Q **Can I use a password manager for my MSK passwords?**

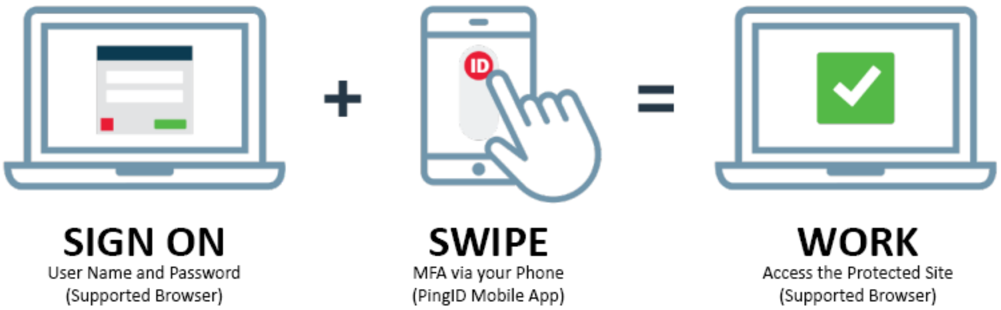
A MSK does not currently support a password management solution. Using a third-party service which MSK does not centrally manage, support, or have a formal business relationship with, opens MSK to the risk of undetected, large scale compromise of key accounts.

Minimum Password Requirements

- At least 8 characters.
- At least one letter.
- At least one non-alphabetic character (Numbers or Symbols).
- Not constructed of a single dictionary word, or something easily guessable.
- Not the same or similar to previous passwords.

KEY POLICY
IT-3025 Access Control Policy
IT-3038 Password Standard

PingID



PingID is MSK's unified login, offering quick and secure access to key resources from anywhere. Don't have a phone with internet access? No problem! PingID also works with YubiKey 5 Security Key's – just insert and tap.

Visit https://mskcc.sharepoint.com/sites/pub-InfoSec/SitePages/MFA.aspx for more information.

Technology, Workflows, and Partnerships: An Evolving Landscape

During your career at MSK, you may be involved with implementing new software or devices or finding new ways to collaborate or share data with outside partners. The Information Security Office has a security risk assessment process which provides leadership and other key decision makers with the information needed to make key risk management decisions in these circumstances.

Engage with Information Security early and often so we can help to manage your IT, data or vendor risk.

Security Risk Assessments

A security risk assessment is required whenever there is:

- An introduction or modification of technology.
- A transfer of MSK data to third-parties.
- Third-party access to MSK information resources

KEY POLICY
IT-3003 Information Security Evaluation Policy