Information Resources: Rules of Behavior

These rules of behavior pertain to all users—Mathematica employees, contractors, and other affiliated personnel—regarding the appropriate use of Mathematica's information resources. All new users of these resources must read and acknowledge the rules to maintain access to Mathematica's systems, networks, or data. Users must also review the rules annually thereafter, which will be done as part of the yearly training on security awareness.

Because written guidance cannot cover every contingency, users should use good judgment in conjunction with the following practices.

Working with Passwords

You are responsible for all computer activity associated with your log-in credentials. Follow these guidelines to protect your password from disclosure:

- **Do not use easy-to-guess passwords**, such as the word "password," your name, relatives' names, or stand-alone dictionary words.
- **Do not write down your password**.
- **Do not share your password** except for an approved business purpose, such as to enable Information Technology Services (ITS) to troubleshoot issues with your computer.
- **If you must share a password, or if you believe someone has otherwise learned your password, change the password as soon as possible**. Report any possible unauthorized access to the Security Incident Reporting site on SharePoint or via email (SecurityIncidents@mathematica-mpr.com).

Protecting Your Computer and the Mathematica Network

Use the following practices to protect your data and information resources:

- **Always log off or lock your computer anytime you leave your workstation** by pressing Ctrl-Alt-Del.
- **Do not install or use unauthorized software**, including freeware, shareware, or public domain software, on Mathematica equipment without written authorization from ITS.
- **Observe all software license agreements** as well as federal copyright laws.
- **Do not interconnect the Mathematica network** to other systems or networks without written ITS authorization.
- **Do not change laptop or workstation configurations** without ITS authorization.
- Except for assigned portable media, such as laptops, **do not remove equipment or exchange system components** without ITS authorization.
- **Protect Mathematica computer equipment** from hazards such as damage, liquids, food, smoke, staples and paper clips, and theft.

- **Avoid emailing large attachments** (more than 5 MB).
- **Limit your use of the Internet for nonbusiness activities**; some incidental personal use is acceptable.
- Use good judgment and **comply with Mathematica's social media guidelines** when accessing social media sites.
- **Avoid applications or utilities that access or search the Internet continuously**, and avoid downloading or streaming large files such as video or music clips.
- **Complete Mathematica's annual security awareness trainings** in a timely manner.

Working with Confidential Information

Protecting the confidentiality of sensitive information is a priority for Mathematica. Much of the data we collect are protected by federal and state regulations. Confidential information includes personally identifiable information (PII), protected health information (PHI), or similar data entrusted to us by clients, survey respondents, and partners. It also includes proprietary business information or other sensitive data about Mathematica, our employees, clients, contractors, partners, and vendors.

- **Do not store confidential information on your work computer** unless it's protected from unauthorized disclosure, loss, and alteration.
- **Project data, especially PII and PHI,** should be stored in project-specific, secure network locations, such as the N: drive or secure databases.
- **Do not disclose or discuss confidential information with unauthorized individuals.**
- **Do not store, access, transmit, or process confidential data on personally owned equipment**, such as home desktop computers, laptops, PDA devices and cell phones, and "thumb" drives.
- Unless approved by the ITS director, **do not use third-party applications** or "cloud" storage to store, access, transmit, or process confidential data.
- **Avoid accessing or working with confidential data in public locations.**
- **Do not alter any file, data record, or application** without proper authorization from your supervisor or project team lead.
- **Do not access or research confidential information** relating to any individual, including yourself, unless such access is required for you to perform your work duties. If you are assigned to a task that gives you access to such data, contact your supervisor or project team lead for guidance.
- If another person asks you to access confidential information, verify that the requested access is authorized. **As a rule, you should not use a computer on behalf of another person**.

Confidential Information and External Media

Protect external media at all times to keep confidential information safe from unauthorized access and unintentional disclosure.

- **If you must store proprietary information on external media** (such as external hard drives)**, only use encrypted media supplied by ITS**.
- **Protect external media from hazards such as electrical currents, extreme temperatures, bending, liquids, and smoke**.
- **Ensure that media are secured based on the sensitivity of the information contained, and practice proper labeling procedures**.

- **Retrieve all printouts in a timely manner**. If you cannot determine the originator or receiver of a printout, dispose of it using a cross-cut shredder.
- **Lock external media and printouts with confidential information in desk drawers or filing cabinets**, and keep the keys with you (do not leave them in or near the lock).
- **If you are unsure about secure data handling practices for external media, contact your supervisor or project team lead.**

Access to Mathematica Facilities

Maintain safety in the workplace by adhering to facility and security policies and procedures.

- **Escort and monitor any non-Mathematica personnel** while they are in Mathematica offices, unless otherwise authorized by Facilities.
- **Do not allow anyone to use your physical access badge/keycard**; keep your badge/keycard with you at all times when entering and exiting the facility.
- **Do not leave the doors to Mathematica facilities ajar**; report any observation of this immediately to Facilities (via the receptionist).
- **Report promptly to Facilities** (via the receptionist):
  - **Anyone without a proper security badge/keycard**.
  - **Anyone who enters or exits a secured facility without a visible badge/keycard**.
  - **Anyone who allows another person without a visible badge/keycard to enter the facility**.
- **Promptly report all security incidents to the Data Compliance team site** in Service Now or via email **(SecurityIncidents@mathematica-mpr.com)**.