Vendor Cybersecurity Network Rules

As a user of our systems, you are responsible for maintaining the security of your account and the information it contains. To help ensure the security and integrity of our systems, please follow these guidelines.

Use Strong Passwords

Create passwords that are at least 8 characters long and include a mix of upper and lowercase letters, numbers, and symbols. Avoid using easily guessable information such as birthdates or names. Phrases are highly encouraged. Never share your username and/or password with anyone.

Use Multi-Factor Authentication (MFA)

MFA adds an extra layer of security to your account by requiring a second factor such as a fingerprint or text message in addition to your password. Enable MFA wherever possible to prevent unauthorized access to your account.

Lock Your System When Not in Use

Always lock your system when you are away from your desk, even if only for a few minutes. This prevents unauthorized access to your account and any sensitive information that may be displayed on your screen.

Patch Your System

Ensure that your system is always up to date with the latest security patches and updates. This helps to prevent vulnerabilities and keep your system secure.

Anti-virus/Malware

Anti-virus/malware protection should be installed on all systems, including operating systems that have been designated as end-of-support.

Email and Web Browsing

No personal use of Shorenstein systems or networks (i.e., email or web surfing). Guest networks are provided as needed.

By following these guidelines, you can help to ensure the security and integrity of our systems. Failure to comply with these Vendor Cybersecurity Best Practices may result in disciplinary action, including termination of your account and legal action as appropriate.

If you have any questions or concerns regarding this policy, please contact our support team at ITHelpDesk@shorenstein.com.

Thank you for your cooperation in maintaining the security of our systems.