ELECTRONIC COMMUNICATION AND USE OF TECHNOLOGY

Version:	11.2
Date of version:	09-07-2021
Created by:	IT GRC
Approved by:	Andrew Isztok, Director of Security, Support, Infrastructure and Networking Safeer Hashmi, Manager, Governance Risk & Compliance
Confidentiality level:	Confidential

Change History

Date	Version	Created by	Description of change
01-30-2013	1.0	Kate Edwards	Basic Document Outline
10-27-2014	2.0	Natalya Pastoukh	Additional review and changes per K. Jones and A. Hewitt. Insertion of non-Company-owned equipment and Instant Messages.
11-04-2014	3.0	Natalya Pastoukh	Changes from Version 2 and additional formatting.
04-15-2016	4.0	A. Vizek	General review for content and formatting.
04-17-2017	5.0	D. Fernandez	General Review.
04-19-2017	6.0	A. Vizek	Review and minor updates to contacts.
04-10-2018	7.0	S. Munson	General review and minor updates to contacts.
07-16-2018	8.0	J. Aguiar	General review and minor updates to content
07-22-2019	9.0	A. Olakanye	General review and minor updates to content
12-18-2019	10.0	T. Nguyen	Edit of IM Communications Method
03-31-2020	10.1	N. Patel	Addition of the Security Training Section
04-01-2020	10.2	A. Izquierdo	Changed OS versions
07-20-2020	10.3	A. Villareal	Addition of the Zoom Section - 14
07-22-2020	10.4	F. Khan	Addition of the Kiteworks Section - 15
07-24-2020	10.5	N. Patel	General review and minor updates to section 14 and 15
09-23-2020	10.6	F. Khan	Minor updated to section 12
10-20-2020	10.7	N. Patel A. Fanseu S. Hashmi	Minor update to section 9
02-26-2021	10.8	N. Patel	Removed section on “Kiteworks” and updated section 13 (Microsoft Teams)
04-07-2021	11	G. Hinote	Review and updated section 10 through 14

5-18-2021	11.1	G. Hinote	Minor update to section 4
09-07-2021	11.2	N. Patel	Addition of section 16.1 on Clear Desk Guidelines

Table of Contents

1. Purpose, Scope and Users

This document sets forth guidelines and procedures for the proper use of Huron Consulting Group's (hereafter "the Company") technical resources which include but are not limited to the following: desktop and portable computer systems, Internet and World Wide Web access, voicemail, e-mail, business and personal productivity applications, Intranet, instant messaging, iOS and other handheld communication devices, electronic bulletin boards, and facsimile services. These technical resources enable individuals to quickly and efficiently access and exchange information throughout the Company and externally. When used properly, these resources greatly enhance individual productivity and knowledge.

This applies to all technical resources whether owned or leased by the Company, used on, or accessed from the Company premises, or used for Company's business and operations.

This policy is applicable to all employees and contractors, as well as other users utilizing company paid accounts, subscriptions, or technical services regardless of the use of Company resources or premises.

2. Reference Materials

Employee Handbook
Mobile Device Management Policy

3. Acceptable Use of Technology

Individuals should use the Company's technical resources, described above, with an understanding that these resources are provided for the benefit of the Company's business. Accordingly, individuals should use the Company's electronic resources to further the Company's ability to conduct its business and in a manner that is consistent with performance of their duties and responsibilities. Individuals should never use the firm's electronic resources for personal use in a way that will impede the individual's work or any responsibilities to clients, vendors, suppliers, or colleagues.

All individuals are responsible for ensuring that they use the Company's electronic resources in an effective, ethical, and lawful manner. The Company's data and files, as well as client work product, data and files, are to be stored only on Company-owned or approved independently owned resources which (for employees) utilize the Company's centrally managed enterprise encryption software or on Company systems. The storage of data on non-Company-owned computers is restricted with exceptions being made on a case-by-case basis. All exceptions are contingent on the utilization of encrypted equipment.

Notwithstanding other sections of this policy, individuals using non-Company owned equipment or resources are subject to additional BYOD Guidelines stated in this document.

4. Unacceptable Use of Technology

The Company's technical resources should not be used for personal gain or the advancement of individual views. This includes the use of technical resources for mining or storing cryptocurrency or other hardware-intensive non-work exercises. Individuals who wish to express personal opinions outside the Company, including on the Internet, are encouraged to obtain a personal account with a commercial Internet service provider and to access the Internet without using Company resources. Individuals' postings are not permitted on the Company's intranet and solicitations may not be made through the email system.

Individuals are permitted to use the Company's technical resources for occasional non-work-related purposes during nonworking time (e.g., during breaks and before or after working hours). Use of the Company's technical resources must not interfere with your productivity, the productivity of any other employee or contractor, or the operation of the Company's technical resources.

Individuals may not send e-mail or other communications that either mask their identity or indicate that someone else sent the communication. Individuals should never access any technical resources using another individual's password. Unauthorized review, duplication, dissemination, removal, installation, damage, or

alteration of files, passwords, computer systems or programs, or other property of the Company, or improper use of information obtained by unauthorized means, is prohibited.

Individuals are prohibited from using the Company's resources for the transmission or receipt of any information in violation of federal, state, or local laws or regulations, including trade secrets. Sending, saving, or viewing offensive material is prohibited. The Company reserves the right to block access to any sites in violation of this policy with exceptions subject to approval by Huron Corporate Legal and Human Resources. Messages stored and/or transmitted by computer, voicemail, e-mail, or telephone systems must not contain content that may reasonably be considered offensive to any individual. Offensive material includes, but is not limited to, pornography, sexual comments, sexual jokes or images, racial slurs, gender-specific comments, or any comments, jokes, or images that would offend someone on the basis of his or her race, color, creed, sex, sexual orientation, age, national origin, ancestry, physical or mental disability, veteran status, as well as any other category protected by federal, state, or local laws. Any use of the Internet or intranet to harass or discriminate is unlawful and strictly prohibited by the Company. Violators will be subject to discipline, up to and including termination of employment. .

The Company does not consider conduct in violation of this policy to be within the course and scope of employment or the direct consequence of the discharge of one's duties. Accordingly, to the extent permitted by law, the Company reserves the right not to provide a defense or pay damages assessed against individuals for conduct in violation of this policy.

5. Ownership of and Access to Information - No Presumption of Privacy

The Company respects the privacy of it's employees. However, that privacy does not extend to an individual's work-related conduct or to the use of Company-provided technical resources or supplies, approved individual resources, regardless of who owns the resource, or the Company's computer, voicemail, e-mail, or telephone systems. All data stored on the above-mentioned resources or Company related data on encrypted machines are, and always remain, the property of the Company. In the case of approved personal technical resources, the owner of the device must assume that the Company can wipe the device of all company related data. In the process of protecting company assets/information, personal data may be lost due to technical limitations inherent in the wipe process.

All information, including e-mail messages and files, that is created, sent, or retrieved over the Company's technical resources is the property of the Company, and should not be considered private or confidential. Individuals should not assume a right to privacy regarding any information or file transmitted or stored through the Company's computer, voicemail, e-mail, or telephone systems.

6. Right to Audit Clause

Computer data, voicemail messages, e-mail messages, and other data are readily available to numerous persons. If, during the course of your employment, you perform or transmit work on the Company's computer system, approved individual resources or other technical resources, your work may be subject to audit, investigation, search, and review as applicable by this policy.

Any electronically stored information that you create, send to, or receive from others may be retrieved and reviewed when doing so serves the legitimate business interests and obligations of the Company. Individuals should also be aware that, even when a file or message is erased or a visit to an Internet or Web site is closed, it is still possible to recreate the message or locate the Web site. The Company maintains the right to monitor individual use of technical resources, Company owned or individually owned and approved, and services at any time. The Company reserves the right to audit, inspect and screen all the Company's technical resources and all information contained therein without prior notice to individuals. These inspections and searches may be conducted during or outside business hours and in the presence or absence of the individual. All information, including text and images, may be disclosed to law enforcement or to other third parties without prior consent of the sender or the receiver.

7. Confidential Information

Communications and computer systems are not entirely secure. Others outside the Company may be able to monitor your e-mail, Internet/Web access, communications and systems use. For example, Internet sites maintain logs of visits from users; these logs identify which Company, and even which person, accessed the service. If your work using these resources requires a higher level of security, please ask your supervisor or the IT department for guidance on securely exchanging e- mail or gathering information from sources such as the Internet or World Wide Web.

E-mail messages containing confidential information should include the following statement at the end of the message: *The information transmitted in this e-mail message and attachments, if any, may be attorney-client information, including privileged and confidential matter, and is intended only for the use of the individual or entity named above. Distribution to, or review by, unauthorized persons is prohibited. All personal messages express views solely of the sender, which are not to be attributed to Huron Consulting Group Inc. If you have received this transmission in error, immediately notify the sender and permanently delete this transmission including attachments, if any.*

8. Security of Information

Although you may have credentials to access computer, voicemail, and e-mail of Huron systems, these technical resources belong to the Company, are to be accessible at all times by the Company and are subject to inspections by the Company with or without notice. The Company may override any applicable credentials to inspect, investigate, or search an individual's files and messages. All credentials must be made available to the IT Department if requested. You should not provide credentials to other individuals or to anyone outside the Company, unless approved by the Chief Compliance Officer, and should never access any technical resources using another individual's credentials.

In order to facilitate the Company's access to information on its technical resources, it is unacceptable to create credentials outside of the IT encryption policy to protect any e-mail, voice- mail, or any other files / data stored or exchanged on Company systems without the express prior written permission from the IT Department and your supervisor. As part of this approval, the IT Department will indicate a procedure for you to deposit any password, encryption key or code, or software with the IT Department so that the encrypted or encoded information can be accessed in your absence. Individuals should not open e-mail attachments that arrive anonymously, that have strange subject titles, or that contain multiple forwards. If individuals are unsure about the safety or content of an e-mail attachment, they must consult with the IT Department before opening the attachment.

9. Security Training

Huron recognizes the best line of defense is a well-trained workforce and will provide security awareness, compliance, and other assorted training opportunities. The training program employed by Huron includes both required and optional security training programs. Required training imposes deadlines and lockout restrictions if the training is not completed by the deadline whereas optional training does not have the same lockout restrictions.

Employees must complete information security awareness training, as well as additional training deemed necessary based on job roles and responsibilities, within 30 days after initial hire. Additionally, if deemed necessary based upon job roles and responsibilities, employees and relevant contractors must complete refresher training on at least an annual basis. If a major change occurs after the annual security training has been completed, updated training will be re-issued to all employees and relevant contractors. Examples of a major change include, but are not limited to, a substantial change in: a physical security system; infrastructure of IT security; local, state, or federal regulations regarding information security; or encryption usage. The Chief Compliance Officer (CCO) and IT GRC team will work with Learning and Organizational Effectiveness (L&OE) to ensure that employees meet all required training obligations.

Failure to participate in **required** security awareness and training programs by the prescribed completion date will result in the user being locked out of the system. Temporary access will only be granted after a request is made to IT Support. In the event that training is still not completed, the user will be locked out of the system and managerial and CCO approval will be required to regain access to Huron systems and data. Security awareness and training reminders may also be provided in the form of periodic e-mails, newsletters, internal website content or posters. In all cases, Huron will retain records of security awareness and training materials delivered as a part of its compliance program.

10. Bring Your Own Device (BYOD)

The Company recognizes that some of the employees and independent contractors will provide their own equipment for use with Huron Consulting Group technology. Cell phone and other mobile devices must be in compliance with the Mobile Device Management Policy, which outlines the mandatory enrollment of devices in the Enhanced Mobility Solution (Intune). For a full list of details and requirements surrounding the deployment of Intune, please refer to the Mobile Device Management Policy Document. All other endpoint devices (laptops) must abide by the following requirements:

10.1. Encryption

There must be encryption on storage areas where the Company's data is held. The IT Department recommends Microsoft BitLocker. Please note that Microsoft 10 includes BitLocker encryption, and Apple MacOS includes Fire Vault encryption. At the request of a practice manager or engagement leader, Huron can provide an external USB hard drive that is fully hardware encrypted and satisfies the requirement of secured storage. The drive uses a 10-digit PIN to activate.

10.2. Patches

All security patches and system updates must be up to date and set to automatically retrieve new patches and system updates.

10.3. Anti-Virus

Anti-Virus software is mandatory which must be configured to automatically update every hour.

10.4. Password

Any device must be protected by a password which will have a minimum length of 8 characters, contains at least one non-alphabetic character, and should never be shared with other users. In addition, the device must be configured to lock after a set period of time (the standard is 15 minutes) which can be set by the majority of screensavers.

Final approval of any non-Huron owned devices and equipment must be granted by the Director of Network and Security.

11. Copyrighted Materials

You should not copy or distribute copyrighted material (e.g., software, database files, documentation, articles, graphics files, and downloaded information) through the e-mail system or by any other means unless you have confirmed in advance from the Company's General Counsel that the Company has the right to copy or distribute the material. Failure to observe a copyright may result in disciplinary action by the Company as well as legal action by the copyright owner.

12. Software Installation Guidance

If an individual would like to install software on Company computers, the IT Department must be informed and request permission prior to installing any software. Employees are prohibited from installing any software on any Company technical resource without the express prior written permission of the IT

Department via submitted ticket to the Contact Center and approval by the Endpoint Engineering Team. Involving the IT Department ensures that the Company can manage the software on Company systems, prevent the introduction of computer viruses or software otherwise installed to bypass implemented IT Security Controls, and meet its obligations under any applicable software licenses and copyright laws. Computer software is protected from unauthorized copying and use by federal and state law; unauthorized copying or use of computer software exposes the Company and the individual to substantial fines and exposes the individual to imprisonment. Therefore, individuals may not load personal software onto the Company's computer system and may not copy software from the Company for personal use. The Company will cooperate with the copyright holder and legal officials in all copyright matters.

In order to mitigate risks associated with mobile and malicious code, only authorized software is permitted to be used at all times on Huron devices and Huron devices connecting to the Huron network. Any exception to this policy will need to be approved by IT Infrastructure.

13. Outlook Email Access

Employees are given multiple access methods to Huron email. The first access method is the desktop Outlook client. This access method is the standard Outlook software that is installed locally on a Company-owned or approved device. Individuals are not allowed to use the desktop Outlook client on a non-Company resource or unapproved devices and are instead required to use the secondary access method: Outlook Web Access (OWA). The use of the desktop Outlook client also does not extend to external (non-Huron) mailboxes such as client or personal email addresses. These accounts are to be accessed using Outlook OWA or a similar browser-based access technology.

Contractors are given access to use the desktop Outlook client with the assumption that the individual will only use it on actively encrypted hardware (See Section 10) that is Company-owned. Contractors do not have the right to use the desktop Outlook client functionality on any unauthorized devices.

As addressed in the Bring Your Own Device section of this policy document, all mobile phone-based access to Huron email must be provisioned through the enrollment of Huron's Mobile Device Manager, Intune.

All individuals are responsible for treating their access to use all e-mail access methods in a manner that is in compliance with the Company's Code of Business Conduct and Ethics, the Employee Handbook, this policy and all other applicable Company policies.

14. Microsoft Teams

14.1. Instant Messaging Client (IMs)

Employees are given system access to use of Microsoft Teams for IM communications and in some cases, employees have access to other IM clients. Any employee, contractor, intern and/or authorized third party (collectively defined as "IM users") must exercise caution regarding conversation and content. Based on configuration standards across the Company, IM's are retained for 30 days unless a user deletes them.

Any exceptions to this policy must be presented to and approved, in writing, by Huron's Legal Department.

All IM users must adhere to and exercise proper use of any electronic resource, as outlined in this policy and in the Information Security Policy. In addition, communication may not consist of and/or involve any of the following:

- Information supporting any business function not directly in support of Huron business functions and procedures
- Information that is an indication of excessive personal use and which interferes with day-to-day employment responsibilities and duties
- Intimidating, hostile or offensive material relating to sex, gender, race, color, religion, national origin, or disability

14.2. Protected Health Information (PHI)

Employees must use Microsoft Teams for secure sharing of files and folders with internal and external users. It is a required platform when sharing sensitive information such as Personal Health Information (PHI), Personally Identifiable Information (PII), or any other information marked as highly confidential by Huron. However, Microsoft Teams is not to be used a primary repository for files and folders.

14.2.1. Huron to Huron PHI Communication Guidelines

- Do not attach files with PHI to a chat. These files are stored in OneDrive which is not an approved location for PHI.
- Chatting PHI (e.g., account numbers) in the body of a chat is permissible if all parties are authorized and have a business need to view the PHI data. These chats are auto deleted after 30 days.
- Do not post PHI directly into a channel message (a.k.a. posts in a channel) because these messages are persistent until the Team is deleted, or the message is deleted manually.
- All PHI files should be stored in the PHI Library in the SharePoint site associated with the Team. Only users that have an approved business need should be granted access to the PHI library.
- Teams Site Owners must ensure that access is immediately revoked for users who no longer have a need.

14.2.2. Huron-to-External PHI Communication Guidelines

These guidelines are nearly the same as Huron-to-Huron PHI Communication, with a few changes/additions.

- You must set up a separate [External] Team and request guest access. Please find the link here to set up Teams with guest access.
- There is no PHI Library in an External Team. Instead, create a private channel called "PHI External" and invite the appropriate guests to that channel.
- The Teams Site Owners must ensure only authorized people have access to the site and the private PHI External channel.
- The PHI External channel must be deleted as soon as the engagement or project had been completed.

15. Zoom Video Conference – Video Conference Tool for Huron

Employees are given access to Zoom under the Company's Zoom Professional Business License. Each Professional License includes a 500-user meeting capacity along with a 1000-user Webinar component. Any employee, contractor, and/or intern must use the security processes in place for Zoom. This pertains to using Zoom on laptop, tablet, and mobile devices when creating and/or joining meetings. All users will automatically be authenticated by using SSO and Duo on new devices when signing into Zoom. As a security initiative, all Zoom Meetings require a password and unique meeting ID. Additionally, a Security Tool Bar Icon has been enabled by Zoom to make meetings more secure and private.

Zoom's most recent update includes the functions listed below:

- UI updates – Security icon, green encryption shield with data center location click through
- Report a User
- Meeting defaults – password, waiting room, and limited screen sharing

- Other features – host disable multiple device login, unmute consent, cloud recording expiration, tighter Zoom Chat controls, and more

The following in-meeting security capabilities are available to the meeting host and have been adopted as best practice by Huron and Zoom.

- Secure a meeting with encryption
- Create Waiting Rooms for attendees
- Require host to be present before meeting starts
- Expel a participant or all participants
- Lock a meeting
- Screen share watermarks
- Audio signatures
- Enable/disable a participant or all participants to record
- Temporary pause screen-sharing when a new window is opened
- Use a passcode to protect a meeting
- Only allow individuals with a given e-mail domain to join

Recorded Zoom meetings show a legal disclaimer that must be accepted by each attendee. If you are recording a session with non-Huron participants AND you plan to share the meeting externally, you must have attendees register so they can agree to additional terms. Please find the link to Zoom resource page here for more details.

16. Individual Responsibilities

Everyone is responsible for the content of all text, audio, or images that they place or send over the Company's technical resources, as well as for the care of any equipment received and which must also be returned in good working condition. Individuals are responsible to safeguard and secure the Company's technology assets issued and may access only files or programs, whether computerized or not, that they have permission to access. Violations of any guidelines in this policy may result in disciplinary action up to and including termination. In addition, the Company may advise appropriate legal officials of any illegal violations and cooperate in investigations conducted by legal officials.

16.1. Clear Desk Guidelines

HCG employees, inclusive of contractors, will clear and secure their designated workspace at the end of each workday whether Working from Home (WFH) or from an office setting. Designated workspaces will be cleared of all sensitive information which includes but is not limited to documents, business cards, post-it notes or other note cards, removable media, CDs, USB sticks, etc. All sensitive information will be secured in locked cabinets, drawers, or offices prior to stepping away from the workspace.

Employees, including contractors, granted access to the private chat rooms (pods) are not allowed to have electronic devices such as laptops, tablets, e-readers (i.e. Kindle, Nook, etc.) in the pods or facility at large, except for cell phones. Employees, including contractors, may possess their cellphone but cellphone activity is prohibited, except for listening to music.

Sanctions for violations of this policy are contingent on the offense. Any incidents experienced will be reported to Governance, Risk and Compliance (GRC) department via IT Service Desk Ticket. The GRC team will work in conjunction with the Chief Compliance Officer (CCO) to recommend any disciplinary actions depending on the severity of the violation (unintentional vs. intentional) and the type of information at issue (e.g., non-PHI vs. PHI, client data exposure, financial, sensitive, or highly confidential data). Sanctions imposed on an employee may include but are not limited to the following: verbal warning, written reprimand, retraining on policies, reduction of bonus, final warning, suspension and termination.

17. **Questions**

Please contact Information Technology, Human Resources, or the Chief Compliance Officer with further questions.