Electronic Communication and Use of Technology

Version:	12.0
Date of version:	09-13-2025
Created by:	IT GRC
Approved by:	Andrew Iztok, Senior Director of IT Infrastructure, Network & Support
Confidentiality level:	Confidential

Table of Contents

1. Purpose

The purpose of this policy is to establish guidelines and procedures for the proper use of Huron's technical resources. The policy aims to ensure that these technical resources are used effectively, ethically, and lawfully to support Huron's business objectives. This policy outlines acceptable and unacceptable behaviors, helping to protect Huron from legal liabilities, security breaches, and misuse of resources. It also serves to educate all Employees and Contractors and/or Contingent workers (Huron Users) about their responsibilities and the potential consequences of policy violations, thereby promoting a secure and productive work environment.

2. Scope & Users

This document sets forth guidelines and procedures for the proper use of Huron Consulting Group's (hereafter "Huron") technical resources which include but are not limited to the following: desktop and laptop computers, servers, Virtual Desktop Infrastructure (VDI), mobile devices, internet access, voicemail, email, instant messaging, intranet, electronic bulletin boards, and fax services. It also covers all business applications, whether cloud-based, SaaS, on-premises, or hybrid. These resources are provided to support business operations and must be used in compliance with Huron's policies and applicable laws ("technical resources"). This applies to all technical resources whether owned or leased by Huron, used on, or accessed from Huron premises, or used for Huron's business and operations.

This policy is applicable to all Huron users, as well as other users utilizing Huron technical resources.

3. Roles & Responsibilities

Huron has identified responsible parties referenced throughout this document. The following lists those roles and summarizes their responsibilities.

Employees and Contractors/ Contingent workers	Use Huron technical resources ethically, effectively, and lawfully. This includes protecting and returning Huron equipment and data as well as ensuring personal use does not interfere with work or put work systems/data at risk. Adhere to all security policies and procedures and follow guidelines for sensitive information. Report any observed suspicious activities. Only use authorized software.
IT Infrastructure Team	Monitor network activities, implement security controls, manage access, and ensure software updates are applied.
Huron Support Center Team	Provide end-user assistance and guidance on technical issues and the secure use of Huron's technical resources.

Information Security / Governance, Risk, & Compliance (GRC) Team	Develop, implement, and maintain security policies. Provide organizational guidance on secure resource use. Review and approve policy exceptions. Investigate and respond to security incidents. Drive security awareness and training programs.
Managers and Supervisors	Ensure team compliance with policy. Facilitate security training. Monitor resource use within teams. Ensure all employees and contractors are properly identified and qualified for their roles.
Legal and Compliance Team	Interpret and provide guidance on laws, regulations, contracts, etc, where security policies, controls, etc may be necessary. Ensure policies align with legal and compliance requirements. Provide guidance on handling confidential information, privacy, data retention, acceptable monitoring, and investigations.
Human Resources Team / HRBPs	Owns onboarding and offboarding. Distribute policies and requirements of Huron Users in the onboarding process. Maintain records of employee acknowledgments, and address policy violations.

4. Reference Documents

Employee Handbook
Global Information Security Policy
Appendix A: Location-Based Asset and Access Policy
Data Classification and Handling Policy
Policies and Procedures for Protected Health Information
IT Exception Policy
Record and Information Management Policy and Record Retention Schedule
Client Data Management Guidelines
Information Security Third-Party Risk Management Best Practices
Social Media Policy
Workplace Recording Policy and Workplace Recording and Transcription Procedure

5. Acceptable Use Of Technology

Client-managed systems are the preferred environment for storing and processing client data unless there is a clean business purpose or client requirement to bring it to the Huron environment.

Only the Huron environment is appropriate and personal or other third-party environments must not be used since they do not utilize the Company's centrally managed security controls and tools (e.g., EDR, encryption software, DLP, etc.).

Huron Users must use Huron's technical resources exclusively to support the Company's business operations in a manner consistent with their roles and responsibilities. All use of Huron's electronic resources must be effective, ethical, and lawful.

The use of independently owned or third-party systems for handling Huron or client data is strictly prohibited unless explicitly authorized in advance by Huron's Governance, Risk, and Compliance (GRC) team.

Any data stored in the Huron environment including hardware, software or peripherals must comply with the Record Retention Schedule and Record and Information Management Policy. Data that does not need to be retained (e.g., duplicates or temporary copies) should be securely deleted using approved methods upon completion of the engagement, in accordance with applicable regulations and client requirements. Refer Client Data Management Guidelines for more details.

6. Unacceptable Use Of Technology

Huron Users must never use Huron's electronic assets and technical resources for personal use in a way that would impede the individual's work or responsibilities to the company and its clients, vendors, suppliers, or workforce. This includes the potential introduction of malware, viruses, unauthorized software, etc, which can negatively impact the specific system, connected applications/systems, or Huron's network in its entirety.

6.1 Storage and Transmission of Sensitive Data

- The use of non-approved tools to store or transmit sensitive Huron or client data is strictly prohibited. This includes but is not limited to personal email, personal cloud storage, private SFTP/FTPS/FTP servers, and non-enterprise messaging platforms such as SMS, iMessage/RCS, and WhatsApp.
- All Huron Users must adhere to client-issued or industry-specific requirements related to the use of third-party tools and applications on Huron equipment. For example, Huron Users must not use applications restricted by their respective industries, such as TikTok in the federal practice. Client Master Service Agreements (MSAs), Statements of Work (SOWs), and other contractual agreements may dictate further, be sure to read and understand all requirements.
- All Huron Users are only permitted to use AI tools to process confidential/sensitive data if it is approved by Huron (e.g., Copilot) and if there are no client-specific or other regulatory restrictions regarding AI usage.
- Certain regulated data such as (FAR/CUI/ITAR) may only be stored in approved cloud environments such as (AWS Gov Cloud or Microsoft Azure (GCC or GCC High). There may be also certain offshore restrictions for ITAR data.
  See Section 7.14, Cloud Security, in the Global Information Security Policy for further information.

6.2 Personal Use

- Huron's technical resources must not be used for personal gain or the advancement of individual views. This includes activities like mining or storing cryptocurrency, social media / online publications, or other hardware-intensive non-work exercises.
- Occasional light personal use of Huron's technical resources is allowed during non-working hours for activities such as checking news, sports, or weather. For personal activities unrelated to work, it is recommended to use personal devices and avoid using Huron technical resources.
- All Huron Users must avoid downloading and storing of personal files on Huron laptops. Downloading files from unapproved sources can introduce malware and other security threats to the Huron environment. Huron is not liable for any personal data stored on Huron devices, including recovery of personal files from Huron laptops, which will not be facilitated.

6.3 Security Controls

Huron Users are prohibited from attempting to bypass or disable any security controls or tools. This includes, but is not limited to:

- Creating virtual servers on endpoints
- Sharing account logins or passwords
- Disabling anti-virus software
- Removing or altering security configurations
- Establishing unauthorized network connections
- Circumventing web filtering mechanisms
- Using non-Huron or non-client VPNs

Any exceptions to these controls must receive formal approval, as outlined in Section 15 Exceptions.

Proper use of Huron's technical resources is critical for security and compliance. Misrepresenting identity, using someone else's credentials, or accessing, altering, or removing files without authorization is strictly prohibited. Sharing confidential information without approval or violating any laws through system use is not allowed. To prevent data loss, Huron uses monitoring tools like Data Loss Prevention (DLP) and restricts unapproved or unencrypted USB devices.

6.4 Dissemination of offensive materials

Sending, saving, or viewing offensive material is prohibited. 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 Huron.

6.5 Endpoint Devices

Huron Users are limited to one Huron endpoint device, (laptop, VDI or other desktop infrastructure) and must promptly return broken/replaced endpoint devices within fourteen (14) days of receipt of a replacement device. For assistance, please contact the Huron Support Center. After fourteen (14) days, the individual's HR Business Partner and manager are notified. Disciplinary action may be initiated if endpoint devices are not returned after thirty (30) days.

In cases of loss or damage of Huron device, penalties will be applied based on individual circumstances.

Huron-issued devices are assigned to individual Huron Users and are not transferable. These devices must not be shared with or used by non-Huron individuals, including family members, friends, or third parties. This restriction ensures the integrity and confidentiality of Huron's systems and data. Any violation of this policy may result in disciplinary action.

7. Clear Desk & Clear Screen Policy

All Huron Users must keep sensitive materials secured using locked cabinets, drawers, or offices, when stepping away temporarily.

Workspaces must be cleared at the end of each day, whether working from home (WFH) or in the office. This may include but is not limited to documents, business cards, post it notes or other note cards, removable media, CDs, and USB sticks. This includes Huron staff granted access to white rooms , private offices, and open office areas. Staff are not allowed to use electronic devices such as laptops, tablets, or e-readers (e.g., Kindle, Nook) in the pods or facility, except for mobile phones. All Huron Users must lock their computer screens, or log out, when stepping away from their workstations for any duration to prevent unauthorized access to sensitive/confidential information

Instructions for locking screens:

- **For Windows devices:** Press **Windows key + L** or navigate to **Start → Profile Icon → Lock.**
- **For macOS devices:** Press **Control + Command + Q** or go to **Apple Menu → Lock Screen.**

This applies to all locations, including both Huron/client premises and remote work environments, such as at home. Huron IT shall configure an automatic screen lock on all physical and virtual workstations, which activates after a maximum of 5 minutes of inactivity.

Sensitive or confidential information should never be left displayed on screens visible to unauthorized individuals. This includes in public settings, when traveling, using conference rooms/projectors, etc. In open office settings and remote working environments, Huron Users should position their screens to prevent casual viewing by others. Built-in privacy screens are enabled as part of default settings for laptops and physical privacy screens can be provided for laptops which do not possess such capability upon request. Avoid displaying sensitive or confidential information on external monitors when unauthorized individuals/ visitors are present. When working in public or shared environments, always use a privacy filter on your laptop screen to protect sensitive data and ensure access cards are always kept secure and never left unattended.

8. Ownership of & Access to Information

8.1 No Presumption of Privacy

Huron respects employee privacy but does not extend it to work-related conduct or the use of Huron-provided or approved technical resources, regardless of ownership. All data stored on these technical resources, including emails and files, are Huron property, and Huron Users should not assume a right to privacy. For approved personal technical resources, such as mobile phones, Huron can remotely wipe the device of all company-related data. In the process of protecting company assets/ information, personal data stored on Company resources such as laptops may be lost due to technical limitations inherent in the wipe process.

8.2 Right to Audit Clause

Work on Huron's systems or approved resources may be audited, investigated, searched, and reviewed as per this policy. Any electronically stored information created, sent, or received may be retrieved and reviewed to verify that it serves Huron's business interests. Deleted files or messages can be restored, and web browser history can be reviewed. Huron reserves the right to monitor individual use of technical resources at any time and to audit, inspect, and screen all Huron resources and information without notice. Inspections may occur during or outside business hours, with or without the individual's presence. All information may be disclosed to law enforcement or other third parties without prior consent.

9. Confidential Information

Users should be aware that absolute security of communications upon computer systems cannot be guaranteed. Activities such as email, internet browsing, and system usage may be monitored or logged by external parties. For example, websites may track visits and identify the Company or individual accessing their services.

If your work involves handling sensitive or confidential information, consult your supervisor or the IT department for approved secure communication methods. To support these efforts, all outgoing external emails are automatically appended with a confidentiality notice, reinforcing the secure handling expectations for Huron communications.

10. Credential & Encryption Management

All Huron Users may be granted credentials to access Huron's computer systems, voicemail, and email; however, all such technical resources are the sole property of Huron. These technical resources must always remain accessible to Huron and are subject to monitoring, inspection, or access by the Company, with or without prior notice. Huron reserves the right to override any user credentials or encryption to inspect, investigate, or search files, messages, or other data stored on, or transmitted, through its systems.

Sharing login credentials with others, using another individual's credentials, or using a shared login not attributed to an individual, to access any technical resources is strictly prohibited. Access to Huron systems must only occur through authorized credentials assigned to the individual user this includes access to laptops, VDIs, servers, applications, clouds, etc. Exceptions may be granted with prior approval following the policy referred in Section 16 Exception.

To ensure data security and maintain organizational access to data and systems, non-Huron encryption or authentication methods must not be used on Huron IT assets without approval from IT (GRC) and your manager. If approved, the IT Department will provide a procedure for you to document any password, encryption key, code, or software details with IT, so the information can be accessed securely in your absence. For further assistance, please contact the Huron Support Center.

11. Bring Your Own Device (BYOD)

All mobile devices (Android and Apple iOS) must be configured with Huron's Mobile Device Management System (MDM), to access Huron data. To qualify for Mobile Device Management enrollment, a device:

- Must have a PIN or passcode configured
- Must encrypt organizational data

- Remain up to date with OS and software patch application

In the event of a mobile device being lost, stolen, compromised, or failing to meet Huron's security standards, or upon termination, Huron reserves the right to remove the device from MDM and remotely wipe all Huron data from the device using its MDM tool to protect company information.

For information on how to report incidents can be found in the Reporting Procedures for Client Cyber Incidents and Lost or Stolen Device or Contact Huron Support Center: U.S/ Canada 213-444-2448; India 080-37244761.

12. Copyrighted Materials

Huron Users should not copy or distribute copyrighted material (e.g., software, database files, documentation, articles, graphics files, downloaded information, etc.) through e-mail or other Huron systems or by any other means. Failure to observe a copyright may result in disciplinary action by Huron as well as legal action by the copyright owner.

13. Software Installation

All software installations on Huron devices must be authorized and approved by IT to protect from malicious or insecure code, and manage licensing. Huron Users cannot install personal software on Huron devices or copy Huron software for personal use. Please contact the Huron Support Center with questions. All requests for new software applications, including SaaS solutions, must undergo the appropriate review and approval process. Where applicable, this may include completing the procurement process before purchasing, downloading, installing, and/or using. This includes free and open-source software. Refer Information Security Third-Party Risk Management Best Practices document for more details.

14. Use of E-mail, Messaging, Social Media, Internet, and Cloud Services

The use of communication tools such as Microsoft Teams, email, social media sites, and other messaging platforms must comply with this policy and Huron's social media Policy. These tools should be used in a way that supports productivity and must not interfere with an employee's ability to perform their duties or negatively impact the organization. Sensitive, Confidential and highly confidential information must never be shared through any channel that is publicly accessible. Please refer to Global Information Security Policy to understand the relevant regulations

14.1 E-Mail

This section outlines approved access methods, standards, and email security practices.

Huron email must be accessed only through approved and secure methods:

- Outlook desktop client on Huron-managed devices
- Outlook mobile app on Huron MDM-enrolled mobile devices
- Web-based Outlook (OWA)

Use of personal or unauthorized devices to configure Huron email is not permitted. External email accounts, including personal or client-provided, must only be accessed via a web browser not through the Outlook desktop client. Contractors are authorized to use the Outlook desktop client only on Huron-owned, encrypted devices.

Huron Users must use professional judgment in emails, maintaining a respectful tone and concise, role-appropriate signatures. Content should be written with the awareness that it may be shared beyond the original recipients.

To reduce the risk of security incidents, Huron enforces several email safety practices:

- Certain attachment types may be blocked to prevent malware or phishing attempts.
- Do not transmit Protected Health Information (PHI) via email. To comply with HIPAA's and other regulatory requirements, PHI and other sensitive data must be transferred through Huron-approved platforms such as Microsoft Teams or SharePoint. In exceptional circumstances where email is the only option to transmit data, reasonable safeguards must be used, such as the use of forced TLS encryption. For all PHI transfers, users must adhere to HIPAA's minimum necessary standard, which requires users to limit PHI to the minimum necessary to accomplish the intended use, disclosure, or request.
- Be cautious with emails from unknown or unexpected sources. Do not open attachments or click links unless the sender and content are verified.
- Do not respond to any request for Confidential or Highly Confidential Information without verifying the sender's identity and intent. If there is any doubt about the legitimacy of an email, contact IT Support before taking action. For detailed guidance on handling sensitive information, refer Data Classification and Handling Policy

  Ensuring secure and professional email usage is critical. This section outlines the approved methods for accessing Huron email, the professional standards expected in email communications, and the security measures to protect sensitive information. By adhering to these policy measures, Huron Users can help maintain the integrity and confidentiality of Huron's communications.

14.2 Microsoft Team Usage

Microsoft Teams is Huron's approved platform for instant messaging, secure file sharing, and video conferencing. It is the preferred tool for collaborating internally and with external partners, particularly when handling PHI, PII, or Confidential data.

Messages in Teams are retained for 30 days unless manually deleted by the user. When using Teams, Huron Users must comply with the following:

- Follow the Microsoft Teams Guidelines and the Data Classification and Handling Policy.
- Use Teams instead of email for sharing sensitive files.
- Use Teams as the primary platform for video conferencing. When recording or transcribing meetings, follow the Workplace Recording and Transcription Procedure and the Workplace Recording Policy.

Business units subject to regulatory or contractual obligations must ensure those requirements are enforced within their teams. Any exceptions to these controls must follow the process described in Section 15: Exceptions.

All communication tools including Microsoft Teams, email, social media, blogs, and other messaging services must be used in accordance with this Policy and the social media Policy available on iNet. Use of these platforms must not interfere with job responsibilities or impact work performance.

15. Exceptions

Huron recognizes that specific business needs and situations may require exception to this Policy. All exceptions must be submitted as a request via the Risk Exception Request and approved by authorized personnel. Please see the IT Exception Policy.

Exceptions will be assessed against the business case and risks associated with the request. Every non-compliant situation requires a full review of specific information to weigh business needs against information security risks. When an exception is granted, it must be documented and scheduled for periodic review.

16. Enforcement

Violations of this policy may result in Corrective action including, but not limited to, the following:

- Coaching and/or Remedial training
- Disciplinary action up to and including termination

17. Policy Maintenance and Distribution

This policy will be updated as needed and will be reviewed annually and made available to all Huron Users.

Change History

Date	Version	Created by	Description of change
01-30-2013	1.0	K Edwards	Basic Document Outline
10-27-2014	2.0	N Pastoukh	Additional review and changes per K. Jones and A. Hewitt. Insertion of non-Huron-owned equipment and Instant Messages.
11-04-2014	3.0	N 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
05-18-2021	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
05-24-2022	11.3	P. Hausken N. Patel	Reviewed and updated sections 5, 6, 9, and 14.2
06-13-2022	11.4	T. Hall	Annual Review and minor update
06-06-2023	11.5	P. Purohith	Annual review and update
09-05-2023	11.6	P. Purohith	Minor update, added to section 14
09-17-2024	11.7	D.SK	Merged Clear Desk and Clear Screen Policy
09-13-2025	12.0	P. Purohith, A. SV & D. SK	Policy Re-vamp to align with current controls, industry best practices, Huron Policy Management Framework.