the results company

HSO Enterprise Solutions, LLC
Information Security and Systems Acceptable Use Policy

March 2023

350 5th Avenue, Suite 6902 | New York, NY 10118
212.502.3900 | www.hso.com

TABLE OF CONTENTS

ACCEPTABLE USE POLICY

1. OVERVIEW

HSO Enterprise Solutions, LLC's (HSO, or "Company"), intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to HSO's established culture of openness, trust and integrity. HSO is committed to protecting our employees, partners, clients and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

HSO provides its employees the computer hardware, software, and networks necessary to fulfill their job requirements. HSO's computer and electronic communication systems, including voicemail, mobile communications, e-mail, PCs, laptops, and flash drives are intended for the creation, management, and transmittal of business-related information. These systems are to be used for business purposes in serving the interests of the company, and of our clients and partners in the course of normal operations. Please review HSO's Employee Handbook for further details on other Human Resource policies.

Effective security is a team effort involving the participation and support of every HSO employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. PURPOSE

The purpose of this policy is to outline the acceptable use of computer equipment at HSO. These rules are in place to protect you, the employee, and HSO. Inappropriate use exposes HSO to risks including virus attacks, compromise of network systems and services, and legal issues.

3. SCOPE

This policy applies to anyone with authorized access to HSO's systems including but not limited to employees, contractors, consultants, temporary employees, and other workers at HSO (collectively referred to as "Employees" in this policy). This policy applies to all equipment that is owned or leased by HSO.

4. POLICY

4.1 General Use and Ownership

- While HSO's IT Team desires to provide a reasonable level of privacy, users should be aware that Company-issued computers and computer-related hardware are the property of the Company and the data created on such systems remains the property of HSO. Because of the need to protect HSO's network, management cannot guarantee the confidentiality of personal information stored on any network device belonging to HSO.
- The Company reserves the right to inspect, monitor, and review all electronic communications systems, including, but not limited to, email, instant messages, chat, and web browsing without notice to the users, in the ordinary course of business, or when deemed appropriate.
- The Company also reserves the right to inspect, monitor, and review all HSO computing systems, including, but not limited to, HSO laptops, HSO tablets, HSO servers, HSO SharePoint, and HSO OneDrive for Business - without notice to the users, in the ordinary course of business, or when

deemed appropriate. Such audits may include, but are not limited to, installed software, saved files, and web browsing history.

- HSO recognizes that its email system may, from time to time, need to be used for personal reasons. Personal email usage should be limited so that it does not interfere with job responsibilities.
- All information distributed via any electronic communication system to HSO Enterprise Solutions' employees or business partners about products or services are considered intellectual assets of HSO Enterprise Solutions, and are not to be distributed to anyone but the intended recipient.
- Equipment that is essential in accomplishing job duties is expensive and may be difficult to replace. When using HSO Enterprise Solutions property, employees are expected to exercise care, perform required maintenance, and follow all operating instructions, safety standards, and guidelines contained herein.
- Employees must notify their manager immediately if any equipment, machinery, tool, appears to be damaged, defective, or in need of repair. The prompt reporting of equipment problems prevents deterioration of the equipment, as well as possible injury to employees or others.
- The careless, negligent, destructive, unsafe, or improper use, or operation of equipment, can result in disciplinary action, up to and including termination of employment.

4.2 Use of Telephones, Mail, and Company Equipment

Employees are expected to keep personal calls to a minimum during business hours. While at work, employees are to exercise the same discretion in using personal cell phones as is used with Company telephones. Excessive personal calls during the workday, regardless of the type of telephone used, can interfere with productivity and be distracting to others. When personal calls are necessary, employees are asked to limit the length of such calls or handle these calls during non-work time.

Under no circumstances are employees to make any chargeable, non-business calls using Company phones. Call detail records of any Company phone to see if abuse has taken place will be reviewed. Employees should also be aware that our phone lines might be monitored for training or other purposes.

Employees are not to use HSO as a personal mailing address and are not to place personal mail through the postage meter. Employees must obtain their manager's approval to use office equipment for personal use, including, but not limited to, copy machines, fax machines, binding machines, etc.

4.3 Internet Usage

HSO provides Internet access in the corporate office to assist and support the job responsibilities of its employees. All Internet data that is composed, transmitted, or received via HSO's computer communications systems is considered to be HSO property and, as such, is subject to disclosure to law enforcement or other third parties. Consequently, employees should always ensure that the business information contained in Internet e-mail messages and other transmissions is accurate, appropriate, ethical, and lawful.

Data that is composed, transmitted, accessed, or received via the Internet should not contain content that could be considered discriminatory, offensive, obscene, threatening, harassing, intimidating, or disruptive to any employee or other person. Examples of unacceptable content may include, but are not limited to, sexual comments or images, racial slurs, gender-specific comments, or any other comments or images that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.

The equipment, services, and technology provided to access the Internet remain at all times the property of HSO. As such, HSO reserves the right to monitor Internet traffic and usage through our online connections.

4.4 Social Media

HSO recognizes that Internet-provided social media can be highly effective tools for sharing ideas and exchanging information. HSO is committed to using social media to promote HSO's visibility and maintain communications with current and prospective employees, customers, business partners, vendors and suppliers, affiliates and subsidiaries, and the general public. HSO is also concerned with ensuring that use of social media serves the Company's need to maintain HSO's brand identity, integrity, and reputation while minimizing actual or potential legal risks.

This policy addresses appropriate use of social media to convey Company information, whether such media is used in or outside the workplace. HSO defines social media broadly to include online platforms that facilitate activities such as professional or social networking, posting commentary or opinions, and sharing pictures, audio, video, or other content. Social media includes personal websites and all types of online communities (for example, Facebook®, LinkedIn®, Yelp®, Pinterest®, YouTube™, Twitter™, Instagram™, Snapchat™, Periscope™, blogs, message boards, and chat rooms).

HSO recognizes that employees might have their own personal social media web pages. As such, HSO respects employees' right to express personal opinions when using personal social media web pages and does not retaliate or discriminate against employees who use social media for political, organizing, or other lawful purposes. HSO encourages employees to link to HSO's external or internal website or social media web pages from personal social media web pages as long as those personal pages follow the employee responsibilities outlined below.

- Personal communications through social media using company equipment, including computers, cell phones and electronic systems, should be limited and not interfere with work responsibilities..
- Employees must abide by all applicable non-disclosure agreements and confidentiality policies of the Company.
- In accordance with Copyright and Trademark regulations, restrictions regarding the use of corporate logos and other branding and identity apply to personal communications through social media. Only individuals officially designated have the authority to speak on the Company's behalf in these forums.

- Employees cannot advertise or sell HSO products via social media websites without prior written approval from a member of HSO's executive team.
- Employee communications, including the transmission of information through social media, are subject to all Company policies, including for example the Company's policy against Discrimination and Harassment.
- Employees are prohibited from making discriminatory, libelous, slanderous or knowingly false comments when discussing the Company, the employee's superior, co-workers, or any other employees of HSO Enterprise Solutions, its management, competitors, or customers.
- The Company reserves the right to take disciplinary action, up to and including termination of employment, against an employee, if any communication is found to violate this policy.

HSO strongly urges employees to use official Company communications to report violations of HSO's Social Media policy, including security breaches, misappropriation or theft of proprietary business information, and trademark infringement. Employees can report actual or perceived violations to their managers, other managers, or to Human Resources.

This policy is not intended to interfere with protected concerted activity or infringe on employee rights under applicable state and federal regulations.

4.5 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of HSO authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing HSO-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.5.1 System and Network Activities

The following activities are strictly prohibited:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by HSO.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which HSO or the end user does not have an active license is strictly prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using an HSO computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any HSO account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Accessing, or attempting to obtain access to, another person's computer, electronic communications or electronic storage without appropriate authorization. Port scanning or security scanning is expressly prohibited unless prior notification to HSO is made.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network or account.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet unless explicitly authorized to do so.
- Providing information about, or lists of, HSO employees to parties outside HSO without a Non-Disclosure Agreement.

4.5.2 Email and Communications Activities

The following activities are strictly prohibited:

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone, or posting online, whether through language, frequency, or size of messages. Examples may include, but are not limited to, sexual comments or images, racial slurs, gender-specific comments, or any other comments or images that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

5. ENFORCEMENT

Any employee found to have violated this policy may be required to attend additional training. Depending on the severity of the violation, disciplinary action may be taken, up to and including termination of employment, however, the policy is not intended to interfere with any protected concerted activity permitted by law.

6. DEFINITIONS

Term	Definition
Personal Blogging	*Writing a personal blog that is not endorsed by HSO. A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption.*
Posting Online	*Writing a comment, question, etc. in an internet hosted publicly accessible location.*
Spam	*Unauthorized and/or unsolicited electronic mass mailings.*
Workforce members	*Employees, volunteers, trainees, and other persons under the direction of HSO.*
Employee	*Paid workforce members.*

DATA SECURITY POLICY

1. PURPOSE

The purpose of this policy is to provide guidance for properly dealing with personal, private, confidential, etc. data. These rules are in place to protect you, the employee, HSO, our clients, and our partners. Inappropriate use exposes HSO, our clients, and our partners to risks including data compromise, data leaks, and legal issues.

2. SCOPE

This policy applies to anyone with authorized access to HSO's systems and HSO's clients' systems, collectively referred to as "Employees". It is especially pertinent to individuals who have access to unscrubbed/non-obfuscated client data.

3. POLICY

3.1 Commitment to Security

Employees must commit themselves to keeping all data secure and shall remain mindful of who has access to client data and how that access has been granted. If a Consultant observes what may be a security breach or issue, they are expected to report the issue to the appropriate people (Project Managers, client contacts, HSO IT staff, etc.).

3.2 Security and Proprietary Information

- All hosts used by the employee that are connected to the HSO Internet/Intranet/Extranet, whether owned by the employee or HSO, shall be continually executing approved virus-scanning checks with a current virus database unless overridden by departmental or group policy.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, as these may contain scams, viruses, e-mail bombs, or Trojan horse code.
- If an employee receives confidential or proprietary data inappropriately, they are to immediately delete the information and request that such information not be sent again in the future.
- Employees shall endeavor to keep proprietary information secure.

3.3 Data Access

Employees shall only work with data that our clients have granted access to. Some employees may only be granted access to scrubbed/obfuscated data and must respect those boundaries. Employees shall not grant data access to other employees or transfer data to non-client systems unless explicitly permitted to do so by the client. Unscrubbed/non-obfuscated data shall not be stored on non-client systems including but not limited to HSO workstations, file servers, SharePoint, OneDrive for Business, personal computers, or personal data storage services.

Security on project collaboration locations (SharePoint project site, OneDrive for Business folders for a project, Microsoft Team location, VSTS code repository, etc.) shall be configured such that only employees working on that project and administrators have access. Do not grant access using anonymous links or to other HSO employees who do not need access to the data to perform their work duties effectively.

3.4 Data Storage

HSO provides secure network locations for data storage including, but not limited to, SharePoint, OneDrive for Business, Code repositories, and corporate file servers. All data considered proprietary or confidential must be stored on corporate servers or cloud hosted systems. Software development code shall be stored in corporate repositories which typically include Team Foundation Server and Visual Studio Team Services. Documents shall be stored in corporate OneDrive for Business, Microsoft Teams, SharePoint repositories, or file shares.

Unless expressly allowed by the client, client databases, data stores, personal data, etc., shall not be removed from the client's system, or stored on personal or HSO workstations, removable devices, or hosted storage services. Such data shall never be stored on personal (Non-HSO and Non-Client) online storage locations such as Personal OneDrive, DropBox, Google Drive, etc.

3.5 Data Transfer

Data transferred across public networks shall be encrypted during the transfer. Acceptable methods include Secure File Transfer Protocol (SFTP), File Transfer Protocol over SSL/TLS (FTPS), HTTPS enabled file transfer tools (SharePoint online, OneDrive for Business, Microsoft Teams, or similar tools), and secure transfer tools authorized by the client. If the client approves, encryption tools may be used to encrypt data before it's transferred over a non-encrypted channel.

Data transfer methods must require authentication. Anonymous access to file transfer methods is not acceptable.

Email between HSO's email system and external email systems shall be considered insecure unless confirmed otherwise by HSO's IT Team.

Reach out to HSO's IT Team if you have questions about how to transfer data securely.

3.6 Data Separation and Classification

Employees must maintain appropriate separation of data for different clients. Designated environments should be maintained for each client to ensure data is not cross contaminated. This includes but is not limited to maintaining designated databases, SharePoint project sites, servers, Office 365 Tenants, and Azure Tenants for each client.

A clear delineation between HSO corporate confidential information, client information, and public information must be maintained. Examples of confidential information include but are not limited to: private corporate strategies, competitor-sensitive information, trade secrets, specifications, customer lists, and research data. Employees must be mindful of these categories of information and take necessary steps to prevent unauthorized access.

Classification of Information:

	Public	Internal Use	Restricted	Confidential
Classification criteria	Making the information public cannot harm the organization in any way	Unauthorized access to information may cause minor damage and/or inconvenience to the organization	Unauthorized access to information may considerably damage the business and/or the organization's reputation	Unauthorized access to information may cause catastrophic (irreparable) damage to business and/or to the organization's reputation
Access restriction	Information is available to the public	Information is available to all HSO employees and selected third parties	Information is available only to a specific group of employees and authorized third parties	Information is available only to individuals in the organization, and stored and transferred using specific controls
Example information assets	• Marketing materials • advertisements, • brochures, • published annual accounts, • Internet Web pages, • catalogues, external vacancy notices	• Departmental memos, • information on internal bulletin boards, • training materials • policies, • operating • procedures, • work instructions, • guidelines, • phone and email directories, • marketing or promotional information • transaction data • productivity reports, • disciplinary reports, • intranet Web pages • Newsletter	• specific customer related information • Technical designs • Service Level Agreements, • contracts, • Sales documents • Licensing • RFC's • Statement of Work (SOW)	• Login credentials • VPN tokens • credit and debit card numbers • personal information (such as employee HR records, Social Security Numbers), • most accounting data • other highly sensitive or valuable proprietary information • PIN codes

3.7 Appropriate Use of Data

Employees shall only use data in a manner required to provide services to the client. Employees shall not export, copy, or process client data for any other purpose.

Use of information Guidelines:

	Public	Internal Use	Restricted	Confidential
Information Asset Types		HSO Internal Corporate Information	Customer Owned Information / Privacy Sensitive Information	Customer Credentials
Handling	**Storage:** No measures required **Transport:** No measures required **Printed copies:** No measures required **Deletion:** No measures required **Retention:** No measures required	**Storage:** Only at locations with appropriate access control measures implemented: Authenticated / Authorized. **Transport:** Amongst Colleagues no restrictions. Across public channels: Use secured (encrypted) transport channels, and address only to authorized recipients. **Printed copies:** only when required. Disposal: destroy to avoid public exposure. **Deletion:** Information should be deleted for active use immediately after completion of the activity of contracted work. **Retention:** According to applicable Laws and regulation, serviced by Backup facilities.	**Storage:** Only at locations with appropriate access control measures implemented: Authenticated / Authorized. Optionally Supported by encryption. **Transport:** Use secured transport channels. (encrypted) **Printed copies:** (if any) never left unattended, destroy after use asap. **Deletion:** Information should be deleted for active use immediately after completion of the activity of contracted work. **Retention:** According to applicable Laws and regulation, serviced by Backup facilities.	**Storage:** Credential set, Only in designated Secure location **Transport:** Use separate media channels to separate username and password. **Printed copies:** Do Not Print at all times **Deletion:** Information should be deleted for active use immediately after completion of the activity of contracted work. **Retention:** According to applicable Laws and regulation, serviced by Backup facilities.

3.8 Notification of Security Breach

Employees must notify appropriate personnel, including creating a case in https://logit.hso.com, immediately of any accidental, unauthorized, or unlawful destruction, loss, alteration, disclosure of, or access to client data ("Security Breach"). Employees are expected to provide as much detail as possible (system affected, type of data, when system was compromised, how system was compromised, etc.) and assist with the investigation/mitigation efforts as requested.

4. ENFORCEMENT

Any employee found to have violated this policy may be required to attend additional security training. Depending on the severity of the violation, disciplinary action may be taken, up to and including termination of employment.

5. DEFINITIONS

Term	Definition
Unscrubbed/non-obfuscated data	Data in its original form that has not been altered to remove personal, private, or confidential information.
Appropriate people to notify	This may include the HSO or Client Project Manager, HSO IT staff, HSO management.
Personal Data	All information relating to an identified or identifiable person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. This may include: name; title; position; employer; contact information (company, email, phone, physical business address and resident address); access / usage / authorization data, contract data, social security number, credit card number, financial data, and bank account data.

WORKSTATION SECURITY POLICY

1. PURPOSE

The purpose of this policy is to provide guidance for workstation security for HSO workstations in order to ensure the safekeeping of information on the device and information the device may have access to.

2. SCOPE

This policy applies to all HSO employees, contractors, workforce members, vendors and agents with an HSO-owned or personal-device connected to the HSO network.

3. POLICY

Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information. HSO will implement physical and technical safeguards for all workstations that access electronic protected information to restrict access to authorized users.

3.1 Workstation Access

- Physical and remote access to workstations shall remain limited to only authorized personnel.
- Keep your workstations with you when traveling. Pack your workstation in your carry-on luggage while traveling by plane, bus, etc. It should not be packed in checked luggage.
- When traveling by car, keep your workstations hidden in your vehicle, i.e. in a covered trunk. Workstations should not be left on a seat for others to see.
- When not in use, workstations should be stored in a safe location, ex. a locked cabinet, hotel safe, space with limited access, using a cable lock, etc.
- Employees must lock their screen when their workstation is not in use.
- HSO highly encourages employees to configure a password protected lock screen with a short timeout on their workstation, and personal and corporate PDAs, tablets, mobile phones, etc.
- Employees are highly encouraged to configure PIN or Fingerprint authentication on personal and corporate PDAs, tablets, mobile phones, etc.

3.2 Workstation Use

- HSO workstations are primarily for HSO corporate use.
- Employees should limit non-corporate use.
- Employees are expected to maintain their own personal computing devices or have access to other means of computing and not depend solely on HSO devices for personal use.
- Personal use of HSO workstations and bandwidth must be negligible and must not interfere with corporate activities.
- Personal use of HSO workstations is subject to all provisions of HSO Information Security and System Usage Policies.

3.3 Password Policies

- It is the employee's responsibility to keep passwords and account credentials secure.
- HSO provides secure password vault software (currently LastPass). This is the only acceptable software for storing credentials.
- Passwords shall not be written down and stored in your workspace or office.

- Employees shall not reveal their password to anyone else, including mangers, technical staff, or household members.
- Corporate credentials are unique to each user and should never be shared.
- If at all possible, non-corporate credentials should not be shared between employees.
- Passwords must be changed if there are indications that the passwords or the system may have been compromised – You are required to report a security incident into LogIT.
- Passwords used for private purposes may not be used for business purposes.
- Passwords must meet the following requirements:
  - Be at least 8 characters long
  - Contain characters from three of the following four categories:
    - Uppercase characters (A...Z)
    - Lowercase characters (a...z)
    - Numerals (0...9)
    - Non-alphanumeric and Unicode characters (!, @, #, $, etc.)
  - Must not contain your first name or last name
  - Is not one of your last three passwords

3.4 Software installation and maintenance

- Employees typically have Administrative access to their systems to facilitate corporate functions.
- Only legally obtained software may be installed on workstations.
- Software should be maintained and updated with current security patches.
- Software installed on workstations must not interfere with corporate activities.
- Workstations are configured for automatic Microsoft Updates, and this feature must not be disabled.
- Employees should be mindful of the Windows Update status on their workstation and shall submit a report to IT if updates are not working properly.

3.5 Data Storage and Recoverability

Data stored on workstations may not be recoverable after a hardware or software malfunction, therefore data should be stored in previously mentioned corporate repositories rather than workstations.

All HSO workstations should have drive encryption enabled. Do not permanently disable such encryption.

3.6 Anti-Virus / Anti-Malware software

- HSO provides corporate grade anti-virus / anti-malware (AV/AM) tools.
- AV/AM tools must remain running at all times.
- Employees should be mindful of the AV/AM status on their workstation and report to IT if the tools are not working properly.

3.7 Public View of Monitors

- Employees must be mindful of others around them.

- Employees should position their monitors in a manner that limits inappropriate viewing of screens.
- Particular care should be taken when using a workstation in public spaces, i.e. airports, airplanes, transit terminals, coffee shops, etc.
- If it is not possible to maintain privacy, employees should refrain from accessing and displaying confidential information on their screen in such locations.
- HSO requires that screens lock after a period of inactivity. Do not bypass this configuration.

3.8 Wireless Networks

- HSO provides encrypted wireless network access within corporate facilities.
- Employees should configure encryption on their personal network at home.
- HSO highly encourages the use of encrypted wireless network access in other locations.
- If it is not possible to use an encrypted wireless network, i.e. a public hotspot, employees are expected to be mindful of the internet resources they access. If possible, use HTTPS versions of websites, encrypted network resources, or connect to HSO's network using a VPN configured to encapsulate all traffic.

3.9 Workstation Loss or Theft

- HSO provides tools to remotely wipe certain device types.
- If necessary, an IT staff member or an employee may initiate a remote wipe of their lost or stolen device.
- Employees are required to report any lost or stolen device that has ever been used to access HSO information, data, or networks, as quickly as possible, and in no case more than 24 hours after such loss or theft is determined
- Employees are required to file a police report in the case of workstation theft and provide a copy of the report to HSO.

4. ENFORCEMENT

Any employee found to have violated this policy may be required to attend additional security training. Depending on the severity of the violation, disciplinary action may be taken, up to and including termination of employment.

5. DEFINITIONS

Workstation/Device	Laptops, desktops, PDAs, tablets, or other computer based equipment containing or accessing HSO information and authorized home workstations accessing the HSO network.
Workforce members	Employees, volunteers, trainees, and other persons under the direction of HSO.
Employee	Paid and unpaid workforce members.

FACILITY SECURITY POLICY

1. PURPOSE

The purpose of this policy is to provide guidance for security related to HSO facilities in order to ensure the safety of employees and safekeeping of information.

2. SCOPE

This policy applies to all HSO employees, contractors, workforce members, vendors and agents with access to an HSO-owned or maintained facility.

3. POLICY

Appropriate measures must be taken when accessing or using facilities to ensure the safety of employees, and the confidentiality, integrity, and availability of sensitive information. HSO will implement physical safeguards and enact policies to prevent access from unauthorized users.

3.1 Facility Access

- Physical access to facilities is limited to authorized personnel only.
- HSO will issue an access badge and/or keys as appropriate.
- Employees shall not share or exchange access badges or keys.
- Employees should refer to the Employee Handbook regarding visitor access to HSO facilities.
- Access to the overall facility and designated areas within it will be granted based on the employee's role within the organization.

3.2 Facility Use

- HSO facilities are primarily for HSO corporate use.
- Employees should limit non-corporate use.
- Personal use of HSO's facilities must be negligible and must not interfere with corporate activities.
- Personal use of HSO's facilities is subject to all provisions of HSO Information Security and System Usage Policies.

3.3 Clean Workspace

- Employees are required to ensure that all sensitive information in hardcopy form is secure in their work area at the end of the day.
- Keys used for access to sensitive information or locations must not be left visible on an unattended desk.
- Printouts containing sensitive information should be immediately removed from printers and fax machines.
- Upon disposal, sensitive documents should be shredded.
- Whiteboards containing sensitive information should be erased when leaving the room/work area.
- Treat mass storage devices such as CDROM, DVD, or USB drives as sensitive and secure them in a locked location.

3.4 Locked Storage

- HSO may provide locked storage locations within HSO facilities as appropriate.
- Employees should request access to a locked storage location if it is appropriate for their role.
- Locked storage may be in the form of a locked room, filing cabinet, etc.
- Employees are highly encouraged to obtain their own locked storage cabinets for home offices if their role requires them to maintain printouts of confidential information.

3.5 Access Badge/Key loss

- Employees are required to immediately report any lost or missing access badge or key.
- HSO can disable access badges at any time as appropriate.
- If required HSO will replace key-based locks to ensure facility security.

4. ENFORCEMENT

Any employee found to have violated this policy may be required to attend additional training. Depending on the severity of the violation, disciplinary action may be taken, up to and including termination of employment.

5. DEFINITIONS

Facility	Physical office, server room, set of cubicles, etc. owned, leased, or generally maintained by HSO.
Workforce members	Employees, volunteers, trainees, and other persons under the direction of HSO.
Employee	Paid and unpaid workforce members.

the results company

USER ACKNOWLEDGMENT FORM

By signing below:

I acknowledge that I have received and read the HSO Enterprise Solutions, LLC ("HSO") Information Security and Systems Acceptable Use Policy. I understand that the policy describes important information about HSO's systems practices. I am familiar with this policy and understand that I am governed by its contents.

I agree that I will maintain familiarity with this policy.

I understand that HSO may, in the future, require an additional signature from me to indicate that I am aware of and understand any new policies, re-issuance of existing policies, and changes to existing policies.

I acknowledge receipt of the HSO Enterprise Solutions, LLC Information Security and Systems Acceptable Use Policy on the date indicated and agree to read it. Should I have any questions, I will contact a member of the IT department.

I understand HSO Enterprise Solutions has the right to amend or modify its contents at any time and that all such modifications will be binding upon all employees.

Employee Name: _____

Signature:_____ Date: _____

This acknowledgement or a copy of it shall be maintained in the employee's personnel file.