The Heritage Group

7.12 THG Acceptable Computer Usage and Security Policy

General Statement of Policy

It is the policy of The Heritage Group (THG) and the responsibility of all users of its computing resources and information assets to:

- Comply with all computer software copyrights and adhere to the terms of all software licenses to which THG is a party.
- Protect the confidentiality, integrity and security of the hardware, data, information, and software applications used by THG.
- Appropriately and effectively use the computing resources and information as required for THG operations and mission.

Administration and Enforcement of the Policy

The THG Corporate IT Group is charged with administering this policy and each THG business unit manager is responsible for its enforcement. Persons are to be made aware of this policy during the hiring process or contracting process and signed copies will be maintained in the employee's master personnel file or supplier contract files.

Penalties and Reprimands
Any user who intentionally violates this Policy will be subject to disciplinary action(s).

Scope of the Policy
This policy applies to users, computing resources and information assets consisting of hardware, software, data, communications process and service providers including but not limited to:

- Users are employees, temporary employees, consultants, and service providers granted access to THG computer resources. Each user is required to read, understand and agree to comply with this policy.
- Hardware includes servers, desktop and laptop computers, tablets, PDAs, cell phones, smartphones, portable drives and storage devices, monitors, printers, routers, modems, switches, and multi-function copy machines and any other devices that will attach directly or indirectly to the THG network or its computing assets.
- Software includes applications that will be loaded onto a hardware device owned by THG or managed on its behalf.
- Data or information that will be stored on a hardware device owned by THG or managed on its behalf that is public, confidential and protected business and personal data, business information, information that is provided by or shared with customers and partners
- Communications include electronic means of communication such as email, blogs, discussion boards, forums and/or online postings.
- Service providers may include managed services providers, systems analysts, hardware break/fix, auditors, contract resources, business analysts, offsite hosting, etc.

Reasonable Care

Users and service providers are to exercise reasonable care with regard to THG computing resources and information assets which includes, but is not limited to:

- Immediately reporting lost or stolen computing resources and/or information assets to the THG IT department.
- Responsibly caring for and safeguarding from damage and theft THG computing resources and/or information assets
- Immediately reporting any breach of security or intrusion by viruses, malware, or other users
- Immediately reporting any misuse of computing resources and/or information assets.
- Immediately reporting any suspicious behavior of other employees or non-employees.

Complying with Licenses and Copyrights

It is the policy of THG to comply with all software and hardware licenses and copyrights.

- **Unauthorized duplication of software may subject users and/or THG to both civil and criminal penalties under the United States Copyright Act.** According to the US Copyright Act, illegal reproduction of software is subject to civil damages of as much as US$100,000 per title infringed, and criminal penalties, including fines of as much as US$250,000 per title infringed and imprisonment of up to five years.
- Users may not duplicate any licensed software or related documentation for use either on THG premises or elsewhere unless THG is expressly authorized to do so by agreement with the licensor.
- Users may not give company software to any outside entities including employees, contractors, customers or others.
- Users may only use software in accordance with applicable license agreements.

Ownership of Data

The following standards apply to ownership of data:

- All data and data files must have an owner who is responsible for the content, access authorization, protection and integrity of the data
- Owners of data are responsible for defining their data's retention and archival requirements and communicating these requirements to IT.
- THG IT is the custodian of business unit data, not the owner of business unit data.

Altering Computer and LAN/WAN Configuration

Users are not permitted to install any software or hardware on any company owned computer without obtaining approval.

- Users are not permitted to alter the hardware configuration of any company provided computer equipment, or LAN/WAN networking device.
- Users are not permitted to disable the anti-virus or other system management services (firewalls, encryption, Windows or other updates, anti-spyware, etc.), or change the configuration of the operatingsystem.
- Users are not permitted to install alternate ISP or WAN data network services into any THG facility.

Hardware and Software

Purchasing Hardware and Software

- **<u>All computer hardware and software purchases must be approved by and/or purchased through the THG IT department.</u>**
- To initiate a purchase request, a detailed request should be sent to the THG IT department help desk, including the account and department to which the equipment is to be charged.
- Employees with procurement card privileges are not to purchase computer hardware or software with these cards without prior approval from the THG IT department.
- Employees must obtain company provided workstations and cannot use personal workstations on THG network.

Registration of Software, Hardware and Services

- All software, hardware and services requiring licenses or implying ownership must be registered in the name of THG or the appropriate business unit. These items must never be registered in the name of an individual user or external service provider.

Disposal of Computing Hardware

- Users need to contact THG IT for scheduling an authorized company to clean and dispose of equipment.

Computer Equipment and Software Personally Owned by a User or Service Providers

Without the prior approval of the ITSS, users and service providers are prohibited from

- Installing software on THG's computers
- Directly attaching computer equipment (laptops, desktops, routers, wireless devices, etc.) to the company network
- Installing company owned software on the user's or service provider's personal computer, tablet or smartphone. The only deviations from this rule pertain to Office 365 installations, permitting users to deploy it on a maximum of 5 mobile devices and 5 computers, and the Workday application, which grants access to functions for employee-self-service functions.

Hardware and Software restrictions

- The use of unauthorized portable storage devices is strictly prohibited on all non-THG external information systems.

Audits

- There will be periodic audits of all THG computer assets to ensure that THG and users are in compliance with all software licenses and this policy and full cooperation of each user is required during an audit.
- THG IT monitors the network and IT assets on a regular basis. If events occur that could jeopardize the availability or security of IT resources or put THG at risk of legal liability, IT will notify appropriate management and could result in disciplinary action.

E-Mail Usage

- All email in, sent by, and received in company email accounts are company property and users should have no expectation of privacy.
- Company email accounts are for business use only and company email addresses should generally not be used to register for personal ecommerce or private communications
- Users must not use the email system for 'spamming', either internally or externally. Spamming is defined as the sending of unsolicited, unnecessary or unwanted emails to other email users.

- All e-mails are to be professional and must not contain inappropriate or offensive content.
- Users should not conduct THG business using third party email accounts like Gmail, Yahoo, etc.
- Users are prohibited from automatically forwarding THG email to a third-party email system (e.g. Gmail, Yahoo, etc.).
- **Email is not archived, and backups are retained only for 30 days. Users must take steps to provide for an archival process if required.**
- Users are prohibited from creating or using PST files. If a PST file is needed, ITSS is required to assist.

Access to Computer Resources

- Access to THG computer resources and data is restricted to authorized users only. Users requiring access to THG technology must be onboarded through the standard HR onboarding processes. Users must also be offboarded through the standard HR offboarding processes to drive the removal of access to THG technology.
- Employees, with manager approval, may grant access to THG computer resources to service providers, customers or temporary employees but this access must be required by a clearly defined business need.
- Access will be granted only for the time needed to perform the task.
- Contract and contingent workers must be registered with THG's HR Shared Services (HRSS) group. This registration process then drives the request and setup of contract and contingent workers' access.
- THG may require multi-factor authentication (MFA) to access company technology resources and/or data. The company's MFA solution is Microsoft Authenticator which must be installed on a company and/or personal mobile device.

Ownership of Stored Documents and Data

- All data and information, including emails, pictures, and other documents, stored on company owned computers, tablets, smartphones, and other devices is the property of the company and users should have no expectation of privacy.
- Data created during one's job/role is property of the company.
- When an employee separates from the company IT can grant access to the former employee's data (e.g. email, OneDrive for Business, etc.) at the request of HR and/or supervisor. This data will be retained for 91 days post separation and then will be deleted.
- Personal data should be stored only on the local computer drive and must not impact the performance of the computer.
- Personally owned documents stored on network storage are subject to deletion at any time and without notice.

Systems and Information Integrity, Security and Confidentiality

It is the responsibility of each user to help maintain the integrity, security and confidentiality of the information and systems that they use or manage.

- Users must not openly post system passwords nor are passwords to be shared with others. Passwords should not be stored on sticky notes or electronic files stored on a user's computer or other company technology resource.
- Users must use the username/password credentials they are assigned and are not to share access.
- Where possible in THG applications, all user account passwords established on internal systems that will contain Heritage data must conform to the following password security requirements:
    - Password expiration = 90 days
    - Password minimum age = 1 day
    - Password history = 8 passwords
    - Minimum password length = 8 characters
    - Passwords complexity must mix alpha, numeric and special characters
    - Maximum invalid login attempts = 3

- Account lockout duration = 15 minutes

- Users are not to install or use any software intended to bypass security measures.
- Users are not to maliciously remove or modify company data.
- Only specific storage devices are backed up by THG IT for recovery purposes. The user is responsible for all information stored on removable media or local (non-server based) storage drives. **Desktops, laptops, tablets and portable drives are not backed up.**
- Users are to comply with all electronic document retention policies as required by their business unit management or by THG policy.
- THG mandates the use of the latest acceptable encryption standards to safeguard data in transit.
- All user endpoints have a maximum operational lifespan of four years, after which they must be evaluated and, if necessary, replaced to ensure compliance with our security standards. Similarly, servers and network hardware are subject to a maximum operational lifespan of five years.
- To ensure that policies and regulations regarding the physical operating environment for organizational assets are strictly adhered to, THG employees will maintain secure physical locations for our servers and workstations, controlling environmental conditions to optimize equipment performance and longevity, and ensure that all physical access to these assets is governed by our comprehensive security protocols.

Data is classified as Confidential, Internal Use or Public. The definition of and handling of this information must conform to the guidance in table below:

		Storage Device or Destination Lower Risk → Higher Risk							
		Network (server/mapped drive, SharePoint, OneDrive for Business)	**Desktop** (local drive)	**Portable Computer** (Local drive on laptop, Tablet)	**Smartphone** (iPhone, Android)	**Email**	**Partner Collaboration Portal** (data room, FTP site)	**Portable Drive** (zip drive, thumb drive, USB drive, and similar)	**Public Cloud** (Cloud drive, Box, OneDrive Personal Dropbox, Google Drive, etc.)
Information or Data Type	**Heritage Confidential Data**	**Allowed**	**Not Allowed**	**Not Allowed**	**Not Allowed** - unless device is encrypted, password protected and document is backed up	**Not Allowed** - unless document is password protected and sent encrypted	**Not Allowed** - unless approved by manager, document is password protected, site is SSL encrypted and document is backed up	**Not Allowed**	**Not Allowed**
	Heritage Internal Use Only Data	**Allowed**	**Allowed**	**Not Allowed**	**Not Allowed** - unless device is password protected and document backed up	**Allowed**	**Not Allowed** - unless approved by manager, document or portal is password protected, site is SSL encrypted and document is backed up	**Allowed but not advised** - device should be encrypted, password protected and document backed up	**Not Allowed**
	Heritage Public Data	**Allowed**	**Allowed – device must be encrypted and password protected**	**Allowed– device must be encrypted and password protected**	**Allowed– device must be encrypted and password protected**	**Allowed**	**Allowed**	**Allowed**	**Allowed**
	Heritage Backup Process	**Daily automatic with 30-day retention**	**No Automatic Backup or not controlled by THG IT**	**No Automatic Backup or not controlled by THG IT**	**No Automatic Backup or not controlled by THG IT**	**Daily automatic with 30-day retention**	**No Automatic Backup or not controlled by THG IT**	**No Automatic Backup or not controlled by THG IT**	**No Automatic Backup or not controlled by THG IT**

Heritage Confidential Data

Any data that contains personally identifiable information concerning any individual and is regulated by local, state, or Federal privacy regulations. Examples include Social Security Number, name with address, banking information, etc. ***NOTE: Credit Cards are considered Confidential Data but are not to be stored electronically.***

Heritage Internal Use Only Data

Any data that is not classified as Heritage Confidential Data, but which is information that Heritage would not distribute to the general public. Examples include financial data, intellectual property, information provided to Heritage by customers, vendors or partners, data declared confidential, contracts and agreements, etc.

Heritage Public Data

Any data that is not classified as Confidential or Internal Use Only and that is already publicly available or Heritage would be comfortable making publicly available.

Internet Use

- Access to the Internet is limited to those users who have a business need. A manager may be required to approve/disapprove a user's Internet access.
- All Internet access is monitored and filtered to prevent abuse and inappropriate content. Users should not access inappropriate content on the Internet such as, nudity, violence, drugs and gambling. Reports of usage will be provided to the appropriate management teams upon request or if abuse is detected.
- Users accessing the Internet are acting as representatives of THG. As such, employees must act in a way that does not damage the reputation of the company or violate the confidentiality, integrity or security of the company computer systems or information.
- Users shall not establish internet email accounts (google mail, yahoo mail, etc.), register URL's, web sites or blogs which could be interpreted to represent the company or would be used to transact company business without prior management approval.
- Users shall not publish any content damaging to the company's reputation, themselves or other individuals within the company on social networking sites, blogs or forums.
- The truth or accuracy of information on the Internet and in e-mail should be considered suspect until confirmed by a separate reliable source.
- Employees shall not place any company material (copyrighted software, internal correspondence, etc.) on any publicly accessible Internet site without a clearly defined business need and prior managementapproval.
- The Internet does not guarantee the privacy or confidentiality of information. Sensitive material transferred over the Internet may be at risk of detection by a third-party and therefore should be sent encrypted. Employees must exercise great caution and care when transferring such material in any form.
- Unless otherwise noted, all software on the Internet should be considered copyrighted work. Therefore, employees are prohibited from downloading software and/or modifying any such files without permission from the copyright holder and compliance with all other licensing requirements.
- 'Shareware' and 'freeware' downloadable from the Internet must be reviewed and installed by the THG IT group.
- Any infringing activity on the Internet by an employee may be the responsibility of THG. Therefore, **THG may choose to hold the employee liable for their actions.**

Social Media

The general use of social media is determined by each business unit. All social media use from THG owned equipment and THG network-connected devices is monitored and filtered by THG IT to prevent abuse and inappropriate content. Excessive use of social media may result in disciplinary actions.
Posting of content to corporate sponsored social media (e.g. the corporate Facebook page) is permitted only for the THG HR Department or as approved by THG HR Department. Please refer to the Electronic Media Policy for further guidance.

Inappropriate Content on Social Media

While social media contains legitimate business and personal content, it also includes content that is inappropriate for the workplace including nudity, violence, drug abuse, sex, and gambling. Therefore, the same inappropriate content policy that applies to the broader Internet use, also applies to content found within social media. Inappropriate content should not be accessed by employees while at work, or while using company resources. Employees should use common sense and consideration for others in deciding which content is appropriate for the workplace.

Mobile Devices
The following standards apply to the use of mobile devices for THG business use: • Only supported mobile devices are authorized for connection to THG systems. Exceptions must be approved by THG IT. • All mobile devices that connect to the THG environment must be registered. • All devices must have the ownership information correctly stored on the device (e.g., your name and telephone number). • Mobile devices containing THG documents or email must be secured with a PIN and device encryption. • THG reserves the right to remove company data from any mobile device.
Artificial Intelligence and Machine Learning
THG has defined a policy around acceptable use of Artificial Intelligence and Machine Learning use in the workplace. Please refer to the AI Use in the Workplace Policy.
Policy Governance Framework
This policy is governed by the NIST Cybersecurity Framework (CSF), which provides a structured approach to managing cybersecurity risk. The framework's core functions of Identify, Protect, Detect, Respond, and Recover guide the development and implementation of this policy to ensure a comprehensive and resilient cybersecurity posture."

Acknowledgement		
I have read THG's Acceptable Computer Use and Security policy and agree to abide by it as consideration for my continued employment by THG. I understand that violation of this policy may result in disciplinary actions and/or revocation of Internet or systems access.		
Employee Signature Section		
Employee Printed Name:	**Employee Signature:**	**Date:**
Manager Approval of Internet Access Signature:		**Date:**