The Acceptable Use of GE Information Resources

Introduction

Information about our Company, our customers, our employees and our suppliers is one of GE's most valuable assets and must be used and protected in an appropriate manner. Similarly, equipment and technology resources belonging to the Company, and provided by GE to its workers, or in some cases, individuals contracted to do work for GE, to process and store information, must also be used and protected appropriately. These Guidelines provide further information under the *Privacy and the Protection of GE Information* and *Security & Crisis Management* policies of The Spirit & The Letter and set out the minimum standards that must be met.

Some GE businesses may have substitute policies and/or additional, specific guidelines in place to meet local or business requirements and these policies and/or guidelines must also be followed where the business policies or guidelines are more restrictive than these Guidelines. Local laws or regulations covering privacy, data protection or information security may also impose additional requirements. To the extent that any statement in these Guidelines would not be permissible under local law, the provisions of local law will prevail.

As a GE worker or contractor with access to such resources, you are responsible for knowing and complying with these Guidelines, *The Spirit & The Letter* and the privacy and information security policies of GE and your business. If you have any questions about your responsibilities, or the application of these Guidelines or your business policies/guidelines, contact your manager, Human Resources or business Privacy or Information Security Leader.

Definitions

GE Information includes all information that is collected or created by the Company, and by you in your GE role — regardless of whether you are working from the office, home or while traveling, and regardless of whether you are working on a GE, personal or third party site or device. For example, personal data that is collected from customers, employees or suppliers, including names, email addresses, phone numbers, account numbers, tax identification or social insurance numbers, is included in the definition of GE Information covered by these Guidelines. GE Information also includes information GE creates in its business processes, such as trade-controlled information, intellectual property and financial information.

GE Information Resources include GE Information and equipment and technology provided by GE to process and store GE Information. For example, computer equipment, fax machines, voice mail, Internet access, email accounts, GE network access, personal data assistants ("PDAs") (e.g, BlackBerries), cellphones and software provided by the Company are GE Information Resources.

Technology evolves continually, and therefore the examples of GE Information Resources provided above are not exhaustive. These Guidelines apply to all GE Information and GE Information Resources regardless of their format or storage media.

Using and Protecting GE Information

WHAT TO KNOW

Different types of GE Information are used for different business purposes and require different levels of protection. GE's Data Classification Guidelines divide GE Information into four categories: Public, GE Internal, GE Confidential and GE Restricted. In addition, the use of customer and supplier data may be governed by contractual agreements between GE and third parties, and the use of personal data is governed by *GE's Commitment to the Protection of Personal Information*, with the use of employee data specifically governed by the *GE Employment Data Protection Standards*. GE workers and applicable contractors are responsible for understanding the relevant guidelines, applicable contracts and local laws that govern the use of GE Information under their control.

WHAT TO DO

LEARN AND COMPLY with policies relevant to your job, including:

- GE Data Classification Guidelines
- GE's Commitment to the Protection of Personal Information
- GE Employment Data Protection Standards
- GE Document Management Procedures and related document retention schedules
- any contractual obligations, such as consumer credit card agreements

RAISE ANY QUESTIONS about the use and protection of GE Information to your business Privacy or Information Security Leader.

USE GE INFORMATION FOR LEGITIMATE BUSINESS PURPOSES and in a manner consistent with the purpose for which the information was initially collected or created.

BEFORE YOU REQUEST OR ACCESS GE Information, ask yourself, "Do I really need this?" Make requests for GE Information following any processes specified in your business, and follow the usage and retention instructions provided by the GE Information owner and the GE Data Classification Guidelines.

CONTROL ACCESS to GE Information and only share it with authorized persons who have a legitimate "need to know" in order to perform their job responsibilities or for other legally authorized reasons. Keep all application login credentials safe. Do not share user IDs and passwords with others. GE Folders and your local file server are considered the best methods for geographically dispersed teams to exchange, store and transport GE Information. Ensure that GE Folders are appropriately access restricted.

MAINTAIN A CLEAR WORKSPACE when you are away from your desk by locking your screen or using password-protected screensavers set at short intervals, keeping confidential materials in a secure place, removing items containing GE Information from fax machines, copiers and scanners in a timely manner, and retrieving physical mail deliveries frequently.

NOTHING IN THIS POLICY PREVENTS YOU FROM REPORTING potential violations of law to relevant government authorities.

WHAT TO WATCH OUT FOR

USES THAT ARE NOT ALIGNED WITH LEGITIMATE BUSINESS PURPOSES, such as sharing customer data with other parties when that sharing is not in compliance with customer contractual agreements.

USING GE INFORMATION RESOURCES AND SPEAKING ABOUT GE INFORMATION in public places, such as airports and restaurants, where people who are not authorized to receive it can overhear your conversations or view your screen, or in open forums on the Internet such as social networking sites.

UNNECESSARY SHARING of GE Information, such as carbon copying ("cc'ing") or bling carbon copying ("bcc'ing") more people than necessary in emails or not appropriately restricting access to GE Folders containing sensitive GE Confidential or GE Restricted information.

IMPROPER DISPOSAL of GE Information, such as tossing GE Information in the trash rather than using a secure method of document disposal. Ask your site manager about secure document disposal and your business Information Security Leader about secure computer file disposal.

STORING GE INFORMATION THAT IS NOT NECESSARY for your current job responsibilities, including information stored on laptops, removable media devices (such as USB drives and external hard drives) and physical documents. Be sure to comply with your business document retention policy and any applicable legal holds; if you have questions about a legal hold, consult your business legal counsel.

GE INFORMATION BELONGS TO THE COMPANY and may not be copied or otherwise removed unless permitted for a legitimate business or other authorized reason. Transition GE Information to your manager or other responsible custodian if you change roles or leave GE.

Using and Protecting GE Information Resources

Your GE Digital Identity

WHAT TO KNOW

Your GE digital identity (for example, your SSO plus password, or other username-password combination) is the key to accessing GE Information and is required for access to GE's network and systems. GE Information is placed at risk of theft or misuse when password protections are compromised, for instance by using shared passwords or by using easy-to-guess passwords or leaving passwords in plain sight.

WHAT TO DO

CREATE ROBUST PASSWORDS, and change them on a regular basis. Do not use common words or phrases, your name, your birthday or your SSO.

NEVER SHARE PASSWORDS, even with someone you trust, such as the Help Desk. If you share your password, you are responsible for any loss, damage or misconduct that arises from its use.

DO NOT POST USERNAMES AND PASSWORDS near your computer. Passwords must be committed to memory.

Portable Devices and Removable Media

WHAT TO KNOW

Portable devices containing GE Information, including laptops, cell phones and PDAs (e.g., smartphones) must be secured at all times. Do not leave portable devices unattended in public. Laptops must be encrypted and physically secured, even in a GE location. GE network access for personally purchased portable or mobile devices must be approved by your business; once granted GE network access, these personally owned devices will be treated as GE Information Resources with respect to approved business-related use, and the device owner becomes responsible for understanding and complying with relevant terms of service.

Removable media (e.g., USB drives, external hard drives, CDs/DVDs) should not be used to store GE Confidential or GE Restricted information unless such devices are encrypted. Personally purchased removable media are not permitted for business use unless expressly permitted by your business. Be aware that if you place GE Information on personal removable media, GE may need to access such devices if required in the context of litigation or other audit or investigation.

WHAT TO DO

LEARN AND COMPLY with these Guidelines, *The Spirit & The Letter* and any business-specific policies and guidelines (which may be more restrictive) addressing the use and protection of portable devices and removable media.

IMMEDIATELY REPORT damage, theft or loss of portable devices or removable media containing GE Information. Follow your business reporting process, and cooperate with related investigations.

RETURN GE Information Resources when they are no longer in use. All devices must be returned for accounting and possible deletion of material. GE Information stored on a personally owned mobile device must be returned to GE when you leave the Company or discontinue business use of that device.

ONLY USE GE REMOVABLE MEDIA for business purposes. Do not use personal devices, such as personally purchased USB memory sticks, which may expose GE Information to greater risk.

WHAT TO WATCH OUT FOR

LEAVING PORTABLE DEVICES IN PLAIN VIEW. If you must leave your laptop in your car, lock it out-of-sight in the trunk.

CROWDED AREAS such as train stations, hotel lobbies, airports and restaurants. Distracting environments create opportunity for thefts.

Using and Protecting GE Information

Internet Access and Email Accounts

WHAT TO KNOW

GE provides Internet access and email accounts for use in business processes. Limited non-business use that is not an abuse of Company time and/or resources, and that does not violate any GE policies applicable to you, is permitted. It is prohibited to use GE Information Resources to access, download, create, display or disseminate material that may be considered obscene, racist, sexist, ageist, physically threatening or similarly offensive, or in violation of any GE policy or guidelines, or may otherwise be perceived to create a hostile work environment.

GE will employ appropriate processes and technologies to protect GE Information Resources from theft and damage. Elements of this protection may include, for example, restricting GE worker or contractor access to the Internet or certain sites or categories of sites, or placing controls on the transfer of GE Information.

WHAT TO DO

LEARN AND COMPLY with these Guidelines, *The Spirit & The Letter* and any business-specific policies and guidelines (which may be more restrictive) addressing Internet access, email use and workplace conduct.

RAISE ANY QUESTIONS regarding the use of Internet access and email accounts with your manager, Human Resources or business Privacy or Information Security Leader.

DO NOT SHARE COPYRIGHTED MATERIAL including music, images, videos or magazines. Downloading or sending copyrighted material through GE Information Resources may infringe the rights of the copyright holder and expose both you and GE to civil and criminal liability. Possession of copyright-infringing materials on GE Information Resources is prohibited.

APPLY THE "NEWSPAPER TEST" before sending an email. Ask yourself, "How would I feel seeing this message reproduced in public?"

DO NOT MODIFY your computer's configuration to circumvent Internet security settings. All GE Web browsers are pre-configured to use specific Internet proxy settings.

WHAT TO WATCH OUT FOR

USE OF PERSONAL EMAIL ACCOUNTS (e.g., Yahoo, Gmail) or calendar systems to conduct GE business is prohibited. GE workers are provided a GE email account for business use.

USING GE INFORMATION RESOURCES FOR ENTERTAINMENT PURPOSES, such as viewing or downloading streaming video or live television broadcasts, is prohibited unless authorized by your manager.

ENGAGING IN NON-GE BUSINESS ACTIVITIES with GE Information Resources is not allowed, even if such business activities are declared in a conflicts of interest statement.

OPENING EMAIL ATTACHMENTS or clicking on links that are suspicious or from an unknown sender. When in doubt, contact your Information Security Leader before accessing such attachments or links.

ACCESSING, DOWNLOADING OR DISTRIBUTING MATERIALS that are in violation of Company policy, including materials that are vulgar, advocate violence or are similarly offensive, or may be perceived as creating a hostile work environment.

USING YOUR GE EMAIL for participating in online social media where your use is primarily personal in nature is permitted, however you should carefully consider the implications of commingling your personal and business lives online before doing so.

Managing Your Online Presence

WHAT TO KNOW

Online Resources, such as GE internal and external blogs, social networking sites and other types of online communities, can be a great way for GE workers to connect with family, friends, colleagues, customers or potential employees — around the globe or down the street . GE sponsors several types of Online Resources — some for employees only, and others available to the general public — and GE employees are encouraged to participate.

Before posting GE Information or your own personal information on Online Resources, it is important to understand the risks, rewards and reach involved. In both your personal and work-related online activity you will need to consider your obligations as a GE employee — including those in *The Spirit & the Letter*, the *Employee Innovation and Proprietary Information Agreement* (EIPIA) and other GE policies, standards and guidelines. Be aware that even personal online activity can be perceived as being connected to GE.

Blogging or posting information, including content, data or files on Online Resources that violates any GE policy, including these Guidelines, *The Spirit & The Letter*, business policies and guidelines, and/or your EIPIA is prohibited.

WHAT TO DO

LEARN AND COMPLY with these Guidelines, *The Spirit & The Letter,* your business policies and guidelines (which may be more restrictive), and applicable laws, including copyright laws.

RAISE ANY CONCERNS about possible security breaches to your manager, Human Resources or business Privacy, Information Security or Communications Leader.

BE ACCURATE AND TRANSPARENT, and if you make a mistake, promptly correct it. Signify when altering a previous post. Remember that the Internet has a long memory, and even deleted postings may be searchable. Never knowingly post false information about the Company's customers, suppliers or competitors.

THINK BEFORE YOU LINK Before inviting a co-worker to connect with you on an external Online Resource, ask yourself if that online connection is appropriate. For example, employees may not feel comfortable with a "friend request" from a manager, and managers may feel uncomfortable with friend requests from members of their teams.

MAKE SURE THAT IT IS ALWAYS CLEAR THAT YOUR VIEWS ARE PERSONAL Do not represent your views as GE's views. Always exercise care before discussing anything related to GE that could expose non-public commercial strategies or intellectual property information, and be aware that even if you do not identify yourself as affiliated with GE, your affiliation may be known to your readers (for example, as a result of your participation on professional or personal networking sites).

WHAT TO WATCH OUT FOR

SPEAKING FOR THE COMPANY without authorization is prohibited. Do not make statements or post information on Online Resources that may reveal non-public details of GE's future business plans or commercial operations. Each GE business has designated professionals who are authorized to speak on GE's behalf and respond to media inquiries. If your activity on an Online Resource may cause you to appear as a knowledgeable GE insider, and reflect on GE, consult with your business Communications Leader for further guidance.

DO NOT USE THE GE MONOGRAM or other GE logos in your personal communications to create the impression that your activity, or information you post, is done on behalf of the Company, unless it is your job to do so.

POSTING ANY TRADE SECRETS on external or personal online resources is prohibited.

DO NOT USE AN EXTERNAL ONLINE RESOURCE AS A MEDIUM FOR COVERT MARKETING which do not identify GE, or you as a GE employee, as the author. If you discuss a GE product or service, or one offered by a competitor, you must clearly disclose your relationship with GE. If you have questions, contact your business Compliance or Communications Leader

PERSONAL ONLINE ACTIVITY that interferes with your work productivity. Do not use GE resources, including work time, for personal online activity beyond limited non-business use.

MAKING PREDICTIVE STATEMENTS that may reveal GE's business strategy or future performance.

BEFORE PARTICIPATING IN ANY SITE, understand who owns the site and what access and security controls apply to the site and any personal or GE Information posted there, and carefully consider if personal or GE content should be posted/shared on that site. Just because a site appears to be GE-branded, GE does not necessarily own or control that site and may not be able to control how content is interpreted, used and protected.

Software and Copyrighted Material

WHAT TO KNOW

GE computers are delivered with standard pre-installed software. Do not disable or uninstall such software. GE will routinely install software on its computers, and any attempt to permanently prevent such software installations is prohibited.

Only software and applications reviewed and approved by your business may be loaded onto GE computers. If you need additional software to perform your job, contact your business Help Desk to follow the applicable business process for approval. The use or installation of software purchased or licensed by GE on any non-GE device is prohibited unless approved by your business Software Governance Leader.

GE may remove or block software that may pose security or compliance risks or conflicts with the operation of GE-loaded software, including freeware, open source software, peer-to-peer file sharing programs, remote control software, voice chat, hacking tools, anonymizers, instant messaging and malware.

WHAT TO DO

LEARN AND COMPLY with these Guidelines, *The Spirit & The Letter,* your, business policies and guidelines, and applicable laws, including copyright laws.

RAISE ANY QUESTIONS regarding the use of software with your business Help Desk or Software Governance Leader.

BE AWARE OF COPYRIGHT RESTRICTIONS. Use of most Internet content, including images found through search engines, requires a license unless labeled as free for commercial use.

WHAT TO WATCH OUT FOR

FREE AND OPEN SOURCE SOFTWARE or applications that may have restrictive licenses. License restrictions can vary depending upon the software's version or usage. Contact your business Help Desk or Software Governance Leader to follow the applicable business processes prior to download on GE computers.

PEER-TO-PEER SOFTWARE OR OTHER FILE-SHARING PROGRAMS. Do not use file-swapping programs on GE computers.

INSTALLING PERSONAL SOFTWARE on GE computers is prohibited unless approved. GE may remove personal software if it poses security or compliance risks or conflicts with the operation of GE-loaded software. GE is not responsible for restoring personal programs or information removed in the process.

INSTALLING GE-LICENSED SOFTWARE on non-GE Information Resources, including personally owned or contractor owned devices, is prohibited unless approved by your business Software Governance Leader.

AUDITS, INQUIRIES OR INFORMATION REQUESTS FROM THIRD PARTIES regarding software license compliance. Do not respond on behalf of your business unless authorized. Immediately contact your business Software Governance Leader if you receive such a request.

Working with Suppliers

WHAT TO KNOW

Protecting GE Information Resources requires close cooperation with suppliers. The *GE Third Party Information Security Policy* and *GE Supplier Acceptable Use of Information Resources* outline the security policies designed to safeguard GE Information from unauthorized or accidental modification, damage, destruction or disclosure when it is in the care of suppliers. But GE workers who work with suppliers must take appropriate precautions before transferring GE Information to suppliers. GE workers are not permitted to release GE Confidential and GE Restricted information to third parties without permission of the GE Information owner, who is the GE employee responsible for the collection or creation of the GE Information, as well as for its protection.

WHAT TO DO

IF YOU WORK WITH SUPPLIERS, LEARN AND COMPLY with the *GE Third Party Information Security Policy* and the *GE Supplier Acceptable Use of Information Resources*.

ONLY SHARE GE INFORMATION ON A "NEED TO KNOW" basis with suppliers.

RAISE ANY QUESTIONS about supplier security with your business Information Security or Sourcing Leader.

SECURE TRANSMISSIONS OF GE INFORMATION to suppliers. Follow business procedures for securing GE Information shared with suppliers, and contact your business Information Security Leader for assistance in selecting and implementing appropriate protections.

WHAT TO WATCH OUT FOR

UNSECURE TRANSMISSION of GE Information to suppliers. All Internet transmissions (e.g., emails) of GE Confidential and GE Restricted information must be encrypted. Contact your Information Security Leader for an appropriate method of transfer.

Compliance with These Guidelines

These Guidelines are designed to protect you, your co-workers and GE. Violation of any portion of these Guidelines may result in disciplinary action, up to and including termination of employment with GE, with respect to applicable law. Violations of these Guidelines by contractors may result in the Company requesting that the contractor's employer remove the contractor from the GE assignment.

GE may review, audit, monitor, intercept, access and disclose information processed or stored on GE Information Resources to ensure compliance with these Guidelines and related GE and business policies and guidelines; to protect the security of GE, maintain proper operations of GE Information Resources, and assure GE compliance with applicable law and regulatory requirements and other business obligations; or for any other reason permitted by local law and/or any local agreements with works councils or unions. If the Company discovers misconduct, including criminal activity or violation of this or any other GE or business policy, any related files or information may be disclosed to authorities.

Raising a Concern

Any concerns about the appropriate use or protection of GE Information Resources should be raised at http://security.ge.com or by contacting your manager, Human Resources, or business Ombudsman or Privacy, Information Security, Software Governance or Compliance Leader.

Links to Other GE and GE Business Guidelines

GE-WIDE GUIDELINES

For an updated list of GE-wide guidelines addressing the use of GE Information Resources, please visit http://security.ge.com.

BUSINESS-SPECIFIC POLICIES AND GUIDELINES

Please note that your GE business may have more stringent policies or guidelines in place affecting your use of GE Information Resources. For an updated list of business-specific guidelines, please visit http://security.ge.com.

Contact Information

If you have any questions about the use of GE Information Resources, please contact your manager, Human Resources or your business' Privacy, Software Governance or Information Security Leader. For a complete list of business contacts, please visit http://security.ge.com.

Revision	3 (supersedes 2013 version)
Issued	January 2016
Effective	January 2016
Document Owner	Christine Sadlouskos
Document Approver	GE Policy Compliance Review Board
Document Classification	GE Internal

Acceptable Use of GE Information Resources Acknowledgment

I acknowledge that I have received the guide to GE Policies Acceptable Use of GE Information Resources.

I understand that every employee is required to comply with the policies described in the guide.

When I have a concern about a possible violation of GE policy, I will raise the concern to a manager, company legal counsel, GE auditor, GE ombudsperson or other compliance specialists.

Name: Rohit Ghosh

SSO ID: 223081407

Signature:

Date: 30-AUG-2022