

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 Security & Crisis Management policies of The Spirit & The Letter and set out the minimum standards that must be met.

Some GE businesses may have additional, specific guidance in place to meet local or business requirements and these must also be met. Local laws or regulations covering privacy, data protection or 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, contact your supervisor, Human Resources or business Privacy or Information Security Leader.

Definitions

GE Information includes all information that is collected or created by the Company. 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 or covered by these Guidelines. GE Information also includes information GE creates in its business processes, such as intellectual property and Company financial data.

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, personal data assistants ("PDAs") (e.g, Blackberries), cellphones and software provided by the Company are GE Information Resources.

Using & 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 employee data is 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 that are relevant to your job or assignment, including:

- GE Data Classification Guidelines
- GE Employment Data Protection Standards
- 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.

ONLY USE GE INFORMATION FOR LEGITIMATE BUSINESS PURPOSES and in a manner consistent with the purpose for which the information was initially collected or created. Misuses of GE Information may be one-time, accidental uses or may include ongoing, routine uses that are outside the original purpose for collection or creation.

BEFORE YOU REQUEST OR ACCESS

GE Information, ask yourself, "Do I really need this?" Only request GE Information necessary to perform your current job responsibilities. 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. 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

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 other people can overhear your conversations or view your screen.

UNNECESSARY SHARING of GE Information, such as carbon copying ("cc'ing") or blind carbon copying ("bcc'ing") more people than necessary in emails or not 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.

Using & Protecting GE Information Resources

Your GE Digital Identity

WHAT TO KNOW

Your GE digital identity (for example, your SSO plus password, your digital certificate, 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 & Removable Media

WHAT TO KNOW

Portable devices, including laptops, cell phones and PDAs (e.g., Blackberries) 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.

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

IMMEDIATELY REPORT damage, theft or loss of GE Information Resources. 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.

ONLY USE GE DEVICES 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.

Internet Access & Email Accounts

WHAT TO KNOW

GE provides Internet access and email accounts for use in business processes. Limited non-business use which is not an abuse of Company time and/or resources and which 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, threatening or otherwise offensive, unprofessional or in violation of any GE policy or guidelines, or may otherwise be perceived to create a hostile work environment.

GE businesses may block potentially objectionable or dangerous Web sites or rely on "content filtering" software to filter broad categories of Web sites. GE cannot review every potentially blocked Web site. The availability or unavailability of a Web site does not necessarily reflect endorsement or censorship by GE. GE may also block streaming media sites (video, music, radio stations) to preserve Internet bandwidth, regardless of content. If a Web site is blocked and needed for a legitimate business purpose, contact your HR manager.

WHAT TO DO

LEARN AND COMPLY with these Guidelines, The Spirit & The Letter and any business-specific guidelines addressing Internet access, email use and workplace conduct.

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

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 supervisor.

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.

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 that are suspicious or from an unknown sender. When in doubt, contact your Information Security Leader before opening such attachments.

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.

ACCESSING, DOWNLOADING OR DISTRIBUTING MATERIALS that are in violation of Company policy, including materials that are non-public, offensive or may be perceived as creating a hostile work environment.

Managing Your Online Presence

WHAT TO KNOW

The use of social media, such as Web logs or “blogs,” peer-to-peer networks and online communities, can be a great way for GE workers to share expertise and perspectives with family, friends, colleagues, customers or potential employees around the globe or down the street. However, it is important to remember that online content reflects not only on your reputation, but on the Company as well.

Before posting information online, it is important to understand the risk, reward and reach involved. If you identify your affiliation with GE or discuss matters related to GE on a Web site forum or blog, you may be perceived as a spokesperson for GE. Any blogging or posting that violates any GE policy, including The Spirit & The Letter and these Guidelines, even when done with personal resources, is prohibited.

WHAT TO DO

LEARN AND COMPLY with these Guidelines, The Spirit & The Letter and applicable laws, including copyright laws.

RAISE ANY QUESTIONS about what is appropriate to your supervisor, Human Resources or business Privacy, Information Security or Communications Leader.

EXERCISE GOOD JUDGMENT when blogging or posting on the Internet or through any electronic means. Be respectful of GE, its officers, employees, customers, partners and competitors. Others may believe your perspective to be an official GE position or opinion.

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 post false information about the Company or its employees, officers, customers or suppliers

CLARIFY THAT YOUR VIEWS ARE PERSONAL by speaking in the first person (“I”). If you identify yourself as in any way affiliated with GE or are known as such, use a prominent disclaimer that your views do not necessarily represent GE. Identify yourself by name and, if you blog or post about GE or GE-related matters, your GE role.

WHAT TO WATCH OUT FOR

SPEAKING FOR THE COMPANY

without authorization is prohibited. Each business has guidelines for speaking on GE's behalf and responding to media inquiries. If your blog may reflect on GE, consult your Communications Leader for further guidance.

DO NOT USE THE MONOGRAM. Do not use any GE logos or trademarks to create the impression that the communication is attributable or approved by the Company, unless specifically authorized to do so.

POSTING ANY NON-PUBLIC/CONFIDENTIAL/PROPRIETARY GE INFORMATION on personal Web sites, blogs or other communications is prohibited.

DO NOT USE A BLOG OR FORUM as a medium for covert marketing or public relations which do not identify GE, or you as a GE worker, 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.

BLOGGING ACTIVITY THAT INTERFERES with your work commitments. Do not use GE work time or resources for blogging unless expressly authorized to do so by your supervisor.

GE EMAIL ADDRESSES should not be used to register with social networking sites, blogs or other sites of a personal nature.

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

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 reviewed and approved by GE Information Security may be loaded onto GE computers. GE may remove additional software that poses a security risk or conflicts with the operation of GE-loaded software. If you need additional software to perform your job, contact your business Help Desk. The use or installation of software purchased and licensed by GE on any non-GE device is prohibited unless you have managerial approval.

GE businesses may block software it deems dangerous, inappropriate or burdensome to the system, including 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, GE's Software Use Guidelines and any business-specific policies.

RAISE ANY QUESTIONS regarding the use of software with your business Information Security 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 SOFTWARE that may have restrictive licenses. Contact your business Information Security Leader or Help Desk before downloading.

INSTALLING PERSONAL SOFTWARE on GE Information Resources. GE Help Desks may remove personal software if it conflicts with operations and are not responsible for restoring personal programs removed in the process.

PEER-TO-PEER SOFTWARE OR OTHER FILE-SHARING PROGRAMS. Never use file-swapping programs on GE Information Resources.

Working With Suppliers

WHAT TO KNOW

Protecting GE Information Resources requires close cooperation with suppliers. The GE Supplier 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. GE workers who interface 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 its protection.

WHAT TO DO

LEARN AND COMPLY with the GE Supplier Information Security Policy and the GE Supplier Acceptable Use of Information Resources.

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

ENSURE SUPPLIER CONTRACTS contain specific obligations to protect GE Information before transferring data. Monitor supplier compliance with such obligations and work with the supplier to correct any deficiencies.

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.

ONSITE CONTRACTORS WITH THEIR OWN EQUIPMENT. If a contingent or contract worker will have access to the GE network for an extended period of time (more than one month), that worker must be provided with GE equipment to perform his or her work functions.

SUPPLIER CONTRACTS THAT DO NOT ADDRESS GE'S HANDLING OF SUPPLIER INFORMATION. Supplier contracts should include any specific obligations GE has with regard to supplier information, including confidentiality and protection provisions.

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, if allowed under 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.

To ensure compliance with these Guidelines, GE may review, audit, monitor, intercept, access and disclose information processed or stored on GE Information Resources if GE has legitimate reason to do so and it is 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 GE business policy, any related files or information may be disclosed to authorities.

Raising a Concern

Any concerns about the appropriate use of GE Information Resources should be raised at <http://security.ge.com> or by contacting your supervisor, Human Resources, Ombudsman, or business' Privacy, Information Security or Compliance Leader. Such concerns may include loss or misuse of a device (e.g., a laptop computer or PDA) or unauthorized sharing or disclosure of GE Information.

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 GUIDELINES

Please note that your GE business may have more stringent 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 supervisor, Human Resources or your business' Privacy or Information Security Leader. For a complete list of business contacts, please visit <http://security.ge.com>.