Privacy and the Protection of GE Information

Issued: September 2010
Supersedes October 2000

integrity.ge.com

Contents

What to know

In today's digital world, information can be shared, stored and accessed in a wider variety of ways than ever before. Whether proprietary information about business plans and operations, or confidential information about employees, customers and suppliers, GE Information is one of the Company's most valuable assets, and must be used and protected in an appropriate manner. The collection, use and protection of information are often regulated. GE is committed to handling information responsibly and in compliance with applicable information security, privacy and other laws.

This responsible handling of GE Information is called Information Governance. Information Governance comprises the set of policies, guidelines and procedures relating to the creation, use, protection and disposal of GE Information Resources. This *Spirit & Letter* policy establishes the principles of Information Governance, and is supported by guidelines and procedures described below, as well as other *Spirit & Letter* policies that involve specific types of personal and business information.

GE may review, audit, monitor, intercept, access and disclose information processed or stored on GE Information Resources to ensure compliance with this policy and its supporting guidelines and procedures; 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.

Definitions

GE Information includes all information that is created or collected 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 this policy. 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, personal data assistants ("PDAs") (e.g., BlackBerries), cellphones and software provided by the Company are GE Information Resources.

GE Documents include all documents and records (paper and electronic) in the possession or control of GE or any of its businesses; this includes documents created by a third party on behalf of GE and documents stored on the Company's behalf by third parties or by you on a personal device. GE Documents may be created or stored within any system, and in any format or media. Some current examples of GE Documents include: email, presentations, spreadsheets, reports, contracts, blog entries, instant messages, calendar entries and handwritten notes.

Technology evolves continually, and therefore the examples of GE Information Resources and GE Documents provided above are not exhaustive. This policy applies to all GE Information, GE Information Resources and GE Documents regardless of their format or storage media.

What to do

Understand that while specific laws, regulations and GE policies may apply to the creation, use and disposal of certain types of GE Information (such as employment, financial or trade-controlled information, or intellectual property), Information Governance principles apply broadly to all information types.

Apply the following principles to the creation and collection of GE information:

- Create or collect GE Information only for legitimate business purposes; only request GE Information needed to perform your current job responsibilities
- Ensure that GE Information is accurate, up to date, and reflects GE Integrity standards; written documents should be fact-based and written in a professional tone
- Classify GE Information according to the GE Data Classification Guidelines

Apply the following principles to the use of GE information:

- Only use GE Information for legitimate business purposes
- Understand the types of GE Information in your control and comply with applicable laws, regulations and GE policies for that information
- Limit access to GE Information to individuals who need it for legitimate business purposes

Learn and comply with the following as they apply to GE Information:

- *GE Data Classification Guidelines*
- *The Acceptable Use of GE Information Resources*
- *GE Employment Data Protection Standards*
- *GE Software Use Guidelines*
- *GE Document Management Procedures*
- Relevant sections of other *Spirit & Letter* policies, including *Controllership*, *Fair Employment Practices, Intellectual Property, International Trade Controls, Security & Crisis Management* and *Supplier Relationships*
- Related business policies, guidelines and procedures
- Laws and regulations governing the collection and use of specific types of GE Information, including but not necessarily limited to personal, financial and trade-controlled information and intellectual property
- Any applicable contractual obligations

Prevent unauthorized access and accidental loss, disclosure or destruction of GE Information by securing GE passwords and devices at all times, and using only GE-approved devices and information storage, transmission and backup tools; secure GE Information in accordance with *GE Data Classification Guidelines*

Manage your online presence by exercising good judgment when posting online. Before posting to any online site, understand how information you post will be used and protected. Remember that online content reflects not only on your reputation, but on the Company as well. Any blogging or posting that violates any GE policy, including other *Spirit & Letter* policies, even when done with personal resources, is prohibited. More information about managing your online presence can be found in *The Acceptable Use of GE Information Resources*.

Do not disable GE pre-installed or GE-deployed software from your GE computer without the express permission of GE IT management. Do not install or use any other software on your computer without business approval. Business applications on GE computers and telecommunications devices are to be managed in accordance with business policy and always in a manner consistent with the *GE Software Use Guidelines*.

Comply with your business document retention policies. Avoid collecting or storing GE Information that is not necessary for your current job responsibilities, but preserve documents and records relevant to pending or foreseeable litigation, investigation or audit (even if you have not received a formal document retention notice) and as directed by Company legal counsel. Always dispose of GE Information securely, for example by shredding or electronic erasure.

Transition essential GE Information to your manager or other responsible custodian if you change roles or leave GE; remember that GE Information belongs to the Company and may not be copied or otherwise removed without permission.

If you learn that GE Information has been used or disclosed in violation of this policy or your business privacy, information governance or other guidelines, or if you learn that the security of any system or device containing GE Information has been compromised, follow your business incident reporting procedure and report the incident at **http://security.ge.com.**

Raise any questions about the use and protection of GE Information to your manager or business privacy, information security, HR or compliance leader, or business legal counsel.

Penalties for violation:

Employees who violate the spirit or the letter of GE's policies are subject to disciplinary action up to and including termination of employment if allowed under applicable law. In addition, if laws are violated, employees or the Company may be subject to criminal penalties (fines or jail time) or civil sanctions (damage awards or fines). GE could also be restricted or prohibited in processing information in the manner necessary to conduct normal business operations.

What to watch out for

Putting GE Information at risk of unauthorized access or accidental loss or disclosure – for example, sharing GE passwords, emailing more people than necessary, uploading GE Confidential or Restricted information (including personal information) to unrestricted Folders/Libraries, or placing GE Information on non-GE approved devices, storage or backup.

Transmitting GE Information without appropriate security controls to suppliers and other third parties. Contracts with third parties must address privacy, information security and other applicable GE requirements for the compliant and secure handling of GE Information.

False or exaggerated statements in email, presentations or other documents. Be aware that documents may travel far beyond an originally intended audience, and have a longevity that far exceeds your tenure at GE or in a particular role. Always write in a professional tone.

Unreported information security incidents. Immediately report any actual or possible compromise of GE Information security to **http://security.ge.com** and follow your business incident response procedure.

What leaders must do

Promote business-specific processes that review and approve new or significantly modified collection, sharing or use of GE Confidential or Restricted information – including where part or all of a process is transitioned to a supplier or other third party. Pay particular attention to GE Information that may be subject to specific requirements, including but not limited to personal, financial or trade-controlled information and intellectual property. Include Privacy, Information Security and other appropriate legal counsel in review, approval and contracting processes.

Be aware of and support business controls designed to prevent, detect and correct inappropriate use or unauthorized access, loss or disclosure of GE Information. Ensure incidents are reported promptly.

Set the example for effective document creation. Create documents that are accurate and maintain a professional tone. Set the record straight where a document or communication may contain inaccuracies or create confusion.

Support the compliant use of software in accordance with GE-negotiated third party license agreements, and ensure that employees are aware of special software licensing considerations for contingent workers and third parties, and special provisions in the event of business acquisitions or divestitures.

Implement effective document management routines, including regularly updated retention schedules, periodic document cleanups, effective transfer of document custodianship for employee role changes or departures, appropriate physical and electronic document disposal procedures and effective document preservation controls. Immediately inform business legal counsel if you become aware of an existing or foreseeable litigation, investigation or audit.

Ensure employees complete business training requirements appropriate to the types and uses of GE Information specific to your business operations.

Lead by example with appropriate use of new technologies such as online resources, social media and collaboration tools. Remember that good judgment always applies, regardless of technology. Inappropriate conduct and communications do not become permissible merely because you are online or using a new technology. Consult with your business privacy, information security or compliance leader or other legal counsel as necessary regarding the appropriate use of new or emerging technologies.

QUESTIONS AND ANSWERS

Q: Am I allowed to visit a social networking site like Facebook while working on my GE computer?

A: Online resources, including Web logs ("blogs"), social networking sites (such as Facebook, LinkedIn, mySpace, Twitter and Yammer) 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. GE has a presence in several of these online resources. Limited non-business use that is not an abuse of Company time and/or resources and that does not violate any GE policies and procedures applicable to you is permitted. But it is important to remember that online content reflects not only on your reputation, but often on GE, as well. It is very important to pay attention to this *Spirit & Letter* policy and its supporting guidelines and procedures, including *The Acceptable Use of GE Information Resources* and its *Managing Your Online Presence* provisions, to help keep both you and GE safe.

Q: What is the most secure way to store the GE Information I am responsible for?

A: Classify and protect GE Information in accordance with the guidance provided in the *GE Data Classification Guidelines* and any applicable business policies, guidelines or procedures, as well as any applicable contractual obligations.

Q: I created a personal document while working on my GE computer – is it GE Information?

A: Limited non-business use of GE Information Resources that is not an abuse of Company time and/or resources and that does not violate any GE policies applicable to you is permitted. Be aware that personal documents created and/or stored on GE Information Resources will be subject to normal business processes that apply to GE Information on those Resources.

Q: What rules apply to GE Information that is created, received or stored on my personal electronic devices?

A: In general, you should restrict GE work to GE devices, as personal devices may expose GE Information to greater risk of loss or unauthorized access. In the limited cases where GE Information is created, received or stored on personal devices, however, be aware that all provisions of this policy and its supporting guidelines and procedures apply to that GE Information.

Q: How can I determine the Dos and Don'ts for software that GE has licensed from a third party?

A: In general, you should first be familiar with the *GE Software Use Guidelines*, and then the training and reference materials prepared by your business for the particular software you use on a regular basis. If you have a question not addressed by these materials, contact your business software governance leader for additional guidance.

Q: Are there special rules I should be aware of regarding certain types of information?

A: Specific laws, regulations or industry standards (such as the Payment Card Industry Data Security Standards, or "PCI DSS") may apply to GE Information you handle in your GE role, including, (for example) personal, financial or trade-controlled information. Your manager and business compliance, privacy and information security leaders and business legal counsel should determine what specific training requirements and business processes and controls apply to these types of GE Information; they can also answer your questions.

Where to learn more

Links

- *GE Data Classification Guidelines*
- *The Acceptable Use of GE Information Resources*
- *GE Employment Data Protection Standards*
- *GE Software Use Guidelines*
- *GE Document Management Procedures*
- *GE Information Security Policy*

Resources

- GE and business Information Governance, Privacy and Information Security practice groups

Related policies, procedures and guidelines

- Controllership
- Security & Crisis Management
- Fair Employment Practices
- Supplier Relationships
- Intellectual Property
- International Trade Controls