GE GDC Induction Training

By: GEGDC Compliance Team

Capgemini

Last updated on 23rd April 2019

Table of Contents

1. Introduction
2. Security Policy
3. Human Resource Security
4. Asset Management
5. Access Control
6. Physical Security
7. Business Continuity Management
8. Incident Management
9. Secure Software Development
10. Information Systems- Audit considerations
11. Communication and Operation Management
12. Data Security & Privacy

Introduction

Welcome to GEGDC Compliance Training!! This training is designed to cover basic compliance controls one should know while working at GEGDC site or GE projects. It is very important and necessary for each resource to know what are the basic modus of operandi while working on GE projects as defined by GE.

- ✓ Being in Service Industry we get access to very sensitive client data
- ✓ GE outsources work to 3rd Parties and there are certain expectations to keep the data secure and safe
- ✓ GE has defined compliance and security requirements for GDC's to follow, so as to enhance value to GE not only with cost-effective solutions but also ensure safe and secure operating environment

Security Policy

Security Policy aims at ensuring uniform and consistent implementation of practice, processes & procedures across all locations covering all functions & services

- There are “20” Security controls as detailed out in the GE GDC Compliance handbook, that serves as backbone for governance model
- Each of these “20” security controls have further sub controls which address specific governance requirement
- Standard Operating Procedures (SOPs are defined for each practice and are available on GDC intranet under CnS Portal)
- Any new release or modification to the SOPs are communicated to GDC employees through emails
- Any tailoring / customization in the process needs approval from Governance Lead / GE IT Risk team, as appropriate

Human Resource Security

GE Onboarding:

- BGC – For initiating GE onboarding, GE-BGC/BGV has to be cleared green for any resources. It is applicable for all employees and Sub contractors.
- Training- It is important for all the resource to get themselves equipped with knowledge of Do's and Don't while working in GE GDC. Hence GE GDC induction is mandatory to be completed before getting access to GE. Within 5 days of onboarding, everyone also needs to complete Understanding Privacy and Software Programming Fundamentals: Software Security Best Practices training program. All the trainings are required to be retaken on annual basis as refresher course.
- PM Role – Upon completion of the above 2 steps, PM can initiate GE onboarding in GDC intranet and inform the SPOC about same
- Access Management – Access to GE GDC can be requested only by respective authorized personnel. PM's initiates onboarding and inform the compliance SPOC's for GE physical and logical access. The SPOC will verify the details entered by PM and requests for GE access.

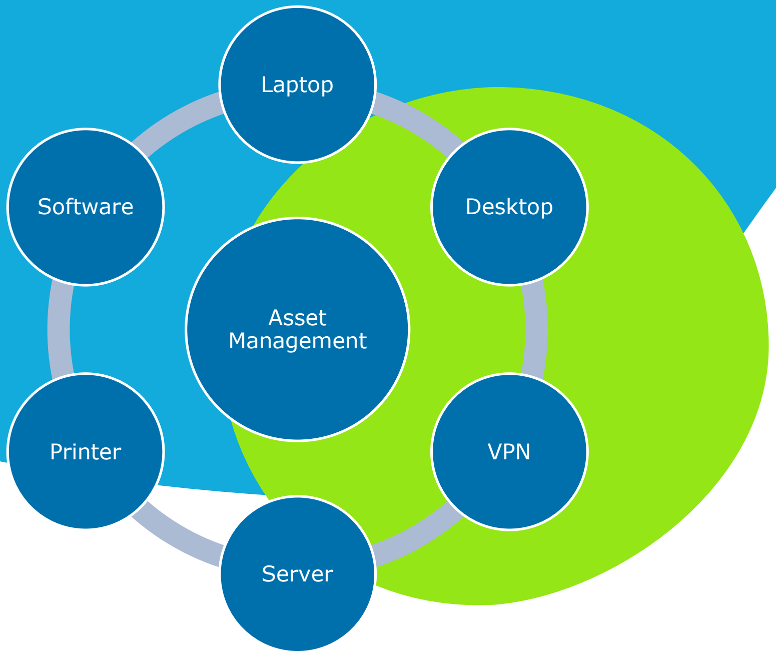
Human Resource Security

GE Offboarding:

- ➢ When the assignment/ project is completed, the resource will be offboarded from GE GDC.
- ➢ Offboarding mandates the PM to complete the below set of key activities

  - ✓ System Formatting
  - ✓ SSOID deactivation(including multiple SSOs)
  - ✓ Inform the on/off boarding SPOC
  - ✓ Any pending tickets reassigned
  - ✓ Surrender of assets
  - ✓ Media Surrender(includes VPN tokens)
  - ✓ Physical & Domain ID Access revocation
  - ✓ SVN Access revocation

Asset Management



Asset Compliance

Any hardware or software owned by GDC is considered an asset, needs to be compliant according to GDC Policies

Compliance

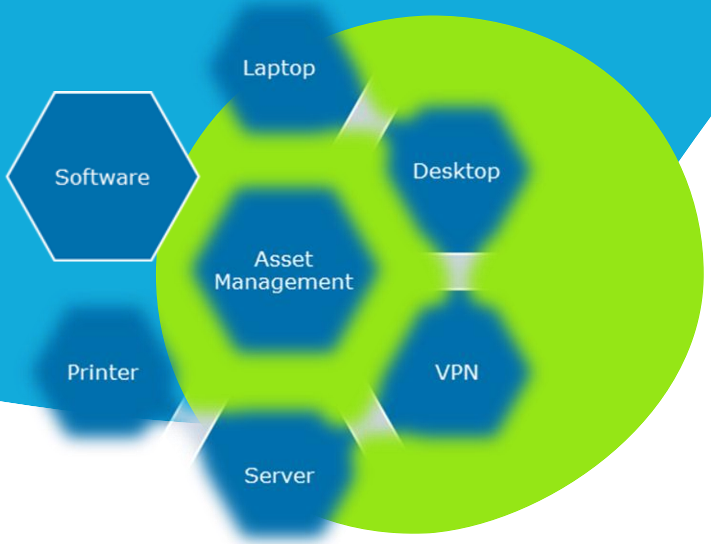
I agree, am responsible

- ➢ All GEGDC Users must be compliant and responsible for appropriate usage and controllership of assets (hardware, software, VPN tokens) which also includes GE supplied assets
- ➢ Ensure protection of Information in the Asset which is paramount and contribute in protection of information by being compliant
- ➢ HAM(Hardware Asset Management) team allocates / de-allocates assets, IT Team supports configuring the system to GDC norms
- ➢ Contribute in Asset compliance by supporting HAM and IT Support team during compliance initiatives
- ➢ Follow the GDC Process for allocation / de-allocation / installation / de-installation of assets based on requirement
  - ➢ To bring or surrendering Customer supplied hardware, one needs to follow the documentation and approval process (Customer + GDC Information Security Leader)

****Approval required from GE Client/Customer + GEGDC IT Governance Leader or ISMS Team + Intimation to HAM team to add the asset in their inventory records – 3 step documented approval**

- ➢ On-time reporting of loss / theft of asset to DL IG CNS cns.ig@capgemini.com
- ➢ Check the GDC Intranet site in your Favorites for **steps to bring customer supplied asset inside GDC**, there is a process

Asset Management



Software Compliance

Only done by authorized personal or system and is monitored for discrepancy

Monitored

All the softwares inside GDC are periodically monitored for authenticity

Software Governance

- Usage of software is tracked and monitored centrally by SAM(**Software Asset Management**) Team
- All SW used inside GDC is authorized and licensed. And is carried out only by Authorized Support Function or tools based on tickets raised in India Service Desk – help.capgemini.com
- Pre-approved freeware for GEGDC users available in every system, which users can install by themselves if required
- Any GE or Client Provided software needs GE(Client/Customer) and GDC Information Security Approved and documented addendum. Only post that, Service desk request(help.Capgemini.com) will be approved by SAM Team for Support function to install
- Every User/PM/DM/Project is responsible for the software installed in their system and should have sufficient details, regarding the ticket raised for the Installation
- Any Un-authorized installation **will be removed** from the system by either Support Functions or tools without intimation
- Users can intimate the IT support, to remove any un-authorized SW if tickets are not available

Asset Management

Software
Laptop
Desktop
Asset Management
VPN
Server
Printer

Softwares from Client

GDC process for client provided software

Software reconciliations

Aids unauthorized software removal

Software Governance

- ➢ Personal software, shareware, open source, evaluation/trialware software are not allowed in GEGDC
- ➢ If these softwares are are required for business purpose, process** needs to be followed
- ➢ Freeware and personal software should not be embedded in production or application delivery
- ➢ Customer supplied software needs to follow the documentation and approval process (Software Governance Leader and Legal approval) 🗎

****Approval required from GE Client/Customer + GEGDC IT Governance Leader or ISMS Team +SAM(Software Asset Management) Team – 3 step documented approval for installation**

NOTE : During reconciliations if it is identified that, any GE Provided software is yet to get extension post end date, will be unbiasedly removed from the system without any intimation. The same can be installed post extension from the client and approved remedy request

Access Control

User Access Management (Single Sign On ID - SSOID):

SSOID is a unique ID provided by GE to access all GE applications and server based on role defined by the GE. Following are the pre-requisite to obtained SSOID:

- ➢ Resource needs to be BGC cleared
- ➢ PM should obtain resources request ID from the GE to raise SSOID
- ➢ Once SSOID is issued to resource, it should not be shared with anyone
- ➢ Upon completion of project or at the time of offboarding SSOID revocation request should be raised on the same day of offboarding
- ➢ Incase VPN access is provided with SSOID, same needs to be surrendered at the time of project closure or offboarding

DO’s & DON’Ts – Physical Security

DO’s

- Physical access to GDC is provided once resource has completed GE on-boarding formalities (GE BGC, Induction training)
- Always wear and display your ID card all the times in the GDC and Capgemini premises
- Please always show your own access card to the card reader at the time of entry and exit even when the door is ajar
- Anti–Pass back” feature has been activated in the Access Control system. So every time you enter / exit the door, flash your access card to the reader, else the door will not open and access violation report will be sent by Security Command Center
- Please acknowledge and respond to the access violation mails sent by Security Command Center
- Follow Clear desk and screen policy in the work area. Confidential and restricted documents must be locked when not in use, and destroyed with a shredder when not needed
- Please ensure entry door is closed once you enter or leave the GDC. If kept open more than 60 secs, the door triggers an alarm to alert the security personnel.
- Any loss or theft of asset must be reported to the CnS team immediately
- GE GDC employee visiting from other GDC locations should raise Multi-location Access request in GDC intranet.
- Report the loss of card immediately to Security Command Center of your location & to CnS team(cns.ig@capgemini.com)
- Be alert and aware. Report any strange, suspicious / unusual behavior/ incidents or events to CnS Compliance Team / Building Security immediately

DO’s & DON’Ts – Physical Security

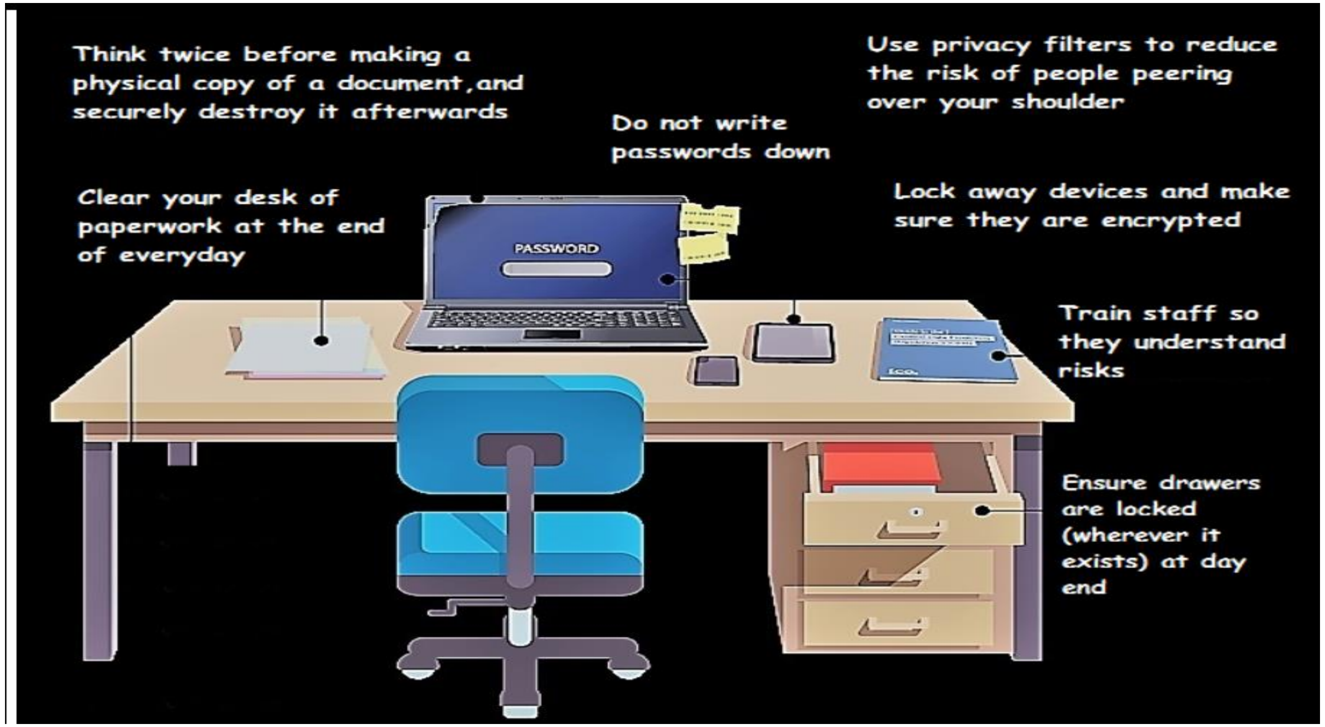
DON’T’s

- **Do NOT** forget to bring / wear your ID card
- Don’t lend your access card to someone else or borrow someone else’s card
- **Photography** and/or video recording via (digital / video / mobile) camera, allowed inside the GDC area including work area, path ways or of any GE confidential document is strictly prohibited
- No electronic devices (like CD, USB, hard disk, Pen drive, digital / video camera) except your mobile device, allowed inside GDC
- Avoid Tailgating or Piggybacking i.e DO not swipe your card for unauthorized person or don’t let any one follow you without swiping the card
- Approvals from GDC Physical Security leader/ Compliance Team are required for every visitors to enter the GE GDC premises
- **Do not allow any Visitors inside GDC without approval.**
- Visitors to be escorted by defined authorized person as per the escort list. Accompany him/her throughout the visit.
- Ensure visitor makes an entry in the visitor register and signed by escort list available with the security.
- Employees not to submit ID card unless GDC work/ formalities are over on Last working day.
- Do not use Fire/ emergency exits for entry/ exiting the GDC. Fire/emergency exits should be used only in case of emergency

Physical Security – Clean Desk Policy

Following a clean desk policy, will help your organization reduce the risk of information theft, fraud, or a security breach caused by sensitive information being left unattended and visible in plain view.

- Employees should keep their desk clean and tidy, with no paper printouts lying near work area
- Ensure no printouts kept lying near the printer bay
- All printouts if not collected by end of the day, will be put in the Trash bin kept near the printer and taken for shredding
- If Printouts are not in use, then it should be shredded


Think twice before making a physical copy of a document, and securely destroy it afterwards
Use privacy filters to reduce the risk of people peering over your shoulder
Do not write passwords down
Clear your desk of paperwork at the end of everyday
Lock away devices and make sure they are encrypted
PASSWORD
Train staff so they understand risks
Ensure drawers are locked (wherever it exists) at day end

Business Continuity Management (BCM)

Every GDC Site has Crisis Management Team (CMT) & Crisis Management Leader (CML) from governance team

- CMT comprises of stakeholders from various departments
- Site CMT details for all locations are uploaded in GDC Intranet and displayed in notice boards
- GDC resources should be familiar with their respective location CMT & contact details
- During any disaster situation, CMT meets & analyzes situation to decide course of action.
- GDC has identified Intracity & Intercity Disaster recovery sites, wherever applicable.

Disaster Management –

- Once CMT declares disaster; communication flows as per call tree documented in the Business continuity Plan
- Fire marshals from each GE GDC locations are identified and trained on how to react to different disaster situation and evacuation procedures
- Fire marshal locations can be identified by an orange cap
- Employee should actively participate in the evacuation drills.

Do’s and Don’ts during Emergency Evacuation Drill

  - Take your keys, purse and critical documents if you can
  - Leave the building using staircases
  - Proceed carefully towards assembly / safe area
  - Be a part of headcount at assembly area
  - Wait for ‘All Clear’ signal before returning to your desk

Information Security Incident Management

Incident – *Any event that compromises Confidentiality, Integrity, availability and safety of employee, or has impact on the delivery of services is considered as an Incident.*

Incident management is a process of identifying events that has impact on the GDC operations, reacting appropriately & responding quickly to minimize the disruption

The risks associated with incidents are further classified as Internal or External risks. Below are some examples of such risks

Material Impact :

Incidents that may cause impact on critical customer services, market share, reputation brands, legal/ contractual requirements can be termed as material incidents
e.g. GE confidential information leakage, copyright infringement etc

Non-Material Impact :

Minor incidents that may not cause major loss and service disruption can be termed as non material incidents e.g. uneven floor

Incident can be reported by –

- Calling location Site CML or GDC CML
- Sending mail to compliance team @ cns.ig@capgemini.com

Secure Software Development (SSD)
Application Security

What is Application Security and its Importance

- Application security is the measure taken throughout the Software Development Life cycle to prevent gaps in the security policy of an application. AppSec Team handles these requirements for all the projects.
- Most of the applications hold sensitive data. This includes, personal, classified and confidential information such as military, financial information and customer feedback.
- Losing these data to competitors, hackers creates huge risk to the business. Hence, it is important to have the application going through code review to ensure that the sanity of the application is well maintained.

Secure Software Development (SSD)
Application Security

Guidelines to be followed for AppSec process

- GE GDC Project teams shall deliver all software's (developed or maintained) that are free of any Critical/High application security vulnerabilities as per GE Guidelines to GE at the time of production releases.
- Applications that are classified as Level 1 / Level 2 and Level 3 risk (High/Medium risk) should ensure GE GDC Secure development Application security assessment is performed.
- All the members the software development team to undergo Secure Development training during Onboarding and refresher training to be taken every year.
- All GDC development (new, maintenance, RTS) details must be entered the GDC intranet portal and GE Support central Workflow portal once the project is initiated.
- All Developers in a GE GDC project team should adhere Secure coding guidelines practice while developing a code and ensure below checklist is incorporated:
    - ❑ Secure code review checklist
    - ❑ Web Secure Application Development checklist.
- GE provided Static Application Security Testing –SAST (Checkmarx/Coverity) and Dynamic Application Security Testing – DAST (HP Web Inspect) tools needs to be used for performing the scans during the development cycle. Registration is done by GE Manager and follow up is done by AppSec team.
- Ensure security issues are fixed before the production releases.

Information Systems Audit Considerations

Internal & External Audits are conducted as per GE Requirements

✓ Periodic Internal Audit conducted by the independent Internal Audit team within GDC

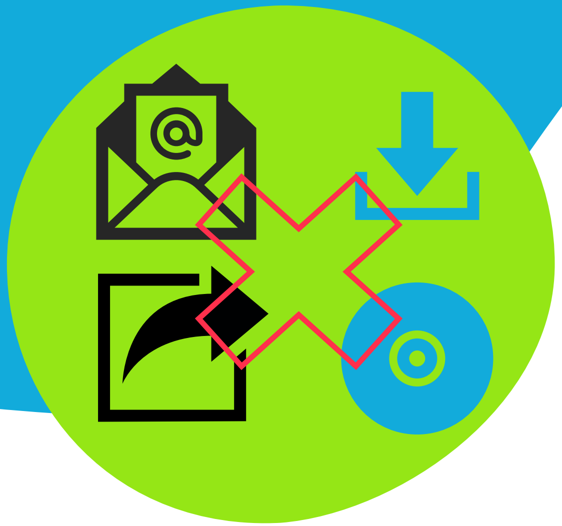
✓ Annual External Audit done by an Third Party Vendor referred by GE

✓ Usually audit period is of one year

✓ Audit findings have to be closed within the stipulated time as agreed upon in remediation details

✓ Employees are requested to co-operate with required information as and when audit notification

Communication and Operations Management



Data Sharing restricted

Violations will be handled with Capgemini's

Stringent policies

Information Classified

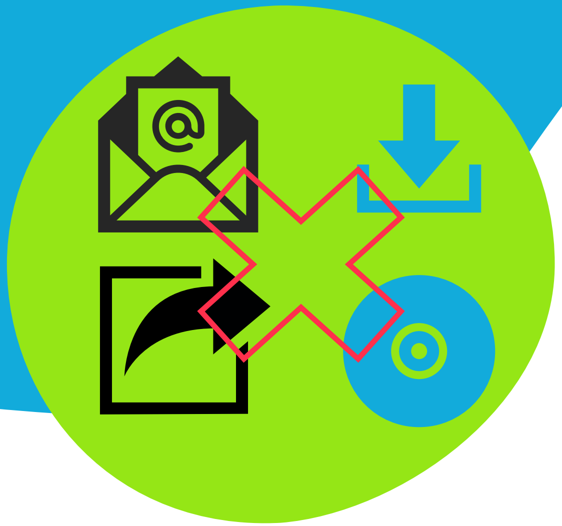
Every user inside GDC responsible for classification of information

CLASSIFIED

GE guidelines recommend to use computing devices such as laptops and desktops for access and not for storage. The purpose of this Security Control is to have secure operating environment to prevent any threat to GE data.

- GE Information is confidential and sensitive hence should not be shared outside GEGDC
- Due to Email DLP, Users are restricted to send any GE classified data to any ID using Corporate email
- DLP implemented – GE Classified document can only be shared with @ge.com from @ge.com email IDs. Or it can be uploaded in the GE Library.
- Basically GE Information should be only within GE boundaries
- Sending GE Confidential / Sensitive / Restricted Classified information to any **personal email or public library**, invites an escalating Auto Incident, which needs to be addressed immediately by Compliance(CnS) team, BU Head, HR Executive, Information Security Management(ISMS) team and Legal Team
- Concerned person will be warned and appropriate action would be taken in accordance to disciplinary action policy as per Capgemini HR norms.

Communication and Operations Management



Airgap ODC

Compliance is critical

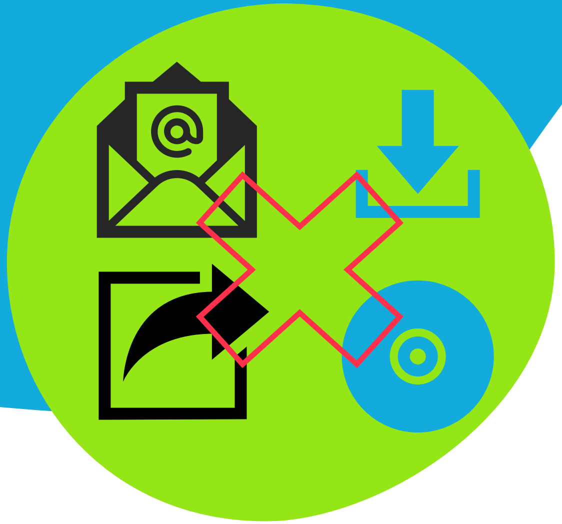
Information is an asset

I am responsible in securing it

GE guidelines recommend to restrict access to users to secure the data in the system

- No proxy edit or Administrator access provided inside GDC
- User to raise exceptions through CNS portal available in favorites and a service request(help.capgemini.com) for action item post approval in CNS portal
- Based on project requirement and client approval, Privilege access is provided to specific application to run in privilege mode using a Group Policy for specific duration of the requirement only
- Users / Projects are responsible for Information in their asset
- Restricted Access to the system with Single sign on enabled
- Remote Desktop not allowed inside GDC from public network
- Desktop sharing restricted

Communication and Operations Management



Authorized Login

Users can login to their system only

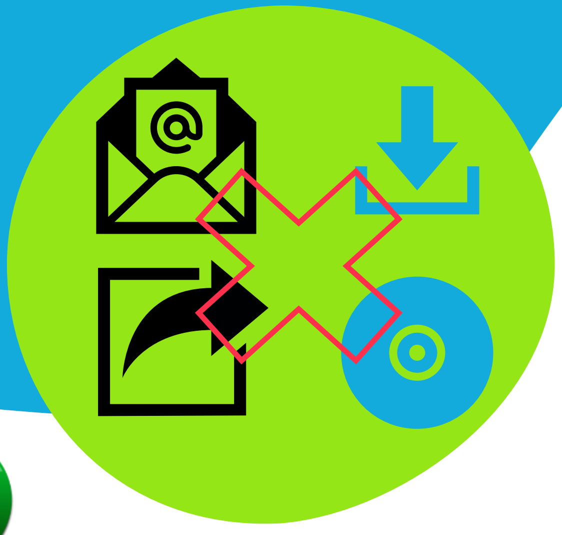
I contribute in compliance

Patches deployed periodically, to avert any threats

Please do not power off or unplug your machine.
Installing update 4 of 11 ...

- **Users are requested to keep their systems online and connected to network**, to ensure critical patches are downloaded as and when pushed or required
- Work From Home users are requested to connect their laptop twice every week inside the ODC, to frequently get updated with regular patch deployments
- No GE data should be stored locally on the system. Any work in progress data should be checked back into GE folders or SVN
- Configuration Managers from each project need to review and update access rights on SVN folder
- All users need to logon onto GDC domain using their credential in their system, un-authorized login is a violation
- Secure printing is enabled to ensure that information does not get printed without authentication
- Users advised to shred the unattended printed papers

Communication and Operations Management



Patch deployment

Secures the system from data hackers

Secure measures

I will co-operate with IT in contributing to secure measures

Yes | No Good

- User / TL / PM responsible for release of asset/logon access during On-site travel. Should follow the GDC process(Format, SVN Access revoke etc)
- GEGDC is a secure environment and has restricted access with transparent control measures.
- Password sharing, un-authorized login, shoulder surfing(peeping into other's desktops), unlocked system, audio recording violate the GEGDC policy, will lead to disciplinary action as per HR policy.
- Users are requested to co-operate periodic and un-planned patch deployments due to periodic scans by GEGDC, securing the asset with compliance initiatives

Data Security

Protection of GE Information from Un-authorized access

- **Data Classification** – To maintain Confidentiality, Integrity, Availability all the data in the system must be classified and will be audited in both Internal and External
- Classification helps us to identify the owner and sensitivity of the information, which helps us to define access control and treatment of information
- All the documents in the system should be classified as per requirement.
- GE Data should be stored in the GE Library, Project related data, source code to be saved in the Central Storage Server(SVN Server)
- GE Data(including PST) is not transferable to Non-GE project in Capgemini or vice versa, systems are formatted
- Unclassified data received from the business should be classified by the user accordingly or stored in GE Library

Classification of Data

Any/all information in an asset needs to be classified

Information classified

I will classify each data

Data Security & Privacy

Protection of GE Information from Un-authorized access is paramount,

- Users are not permitted to store any data on their local systems except the PST files and Work in progress documents (WIP)
- Laptops and emails between Capgemini and GE are encrypted
- Websense End Point DLP implemented across all GDC Assets
- Anti-Spam and Anti-virus installed to protect the system
- Patch deployment download tool installed

Data Privacy –

The importance of protecting privacy, safeguarding personal information and enabling trust. Personal information means information relating to an identified or identifiable person.

If applicable, failure to adequately protect personal data or to comply with global data privacy laws can potentially result in damaged reputations, significant financial and legal penalties, criminal sanctions and the loss of client's and partner's trust.

Data Privacy is every individual's responsibility! We should always adhere to best practices while dealing with personal information.

Compliance

Adhering to core GDC security and global security policies and initiatives helps the projects as well as companies to grow

I Comply

I will responsibly adhere to GDC compliance measures

Watch out for emails from governance leader, for regular compliance awareness updates

For any Compliance & Security related queries, contact CNS (cns.ig@capgemini.com)