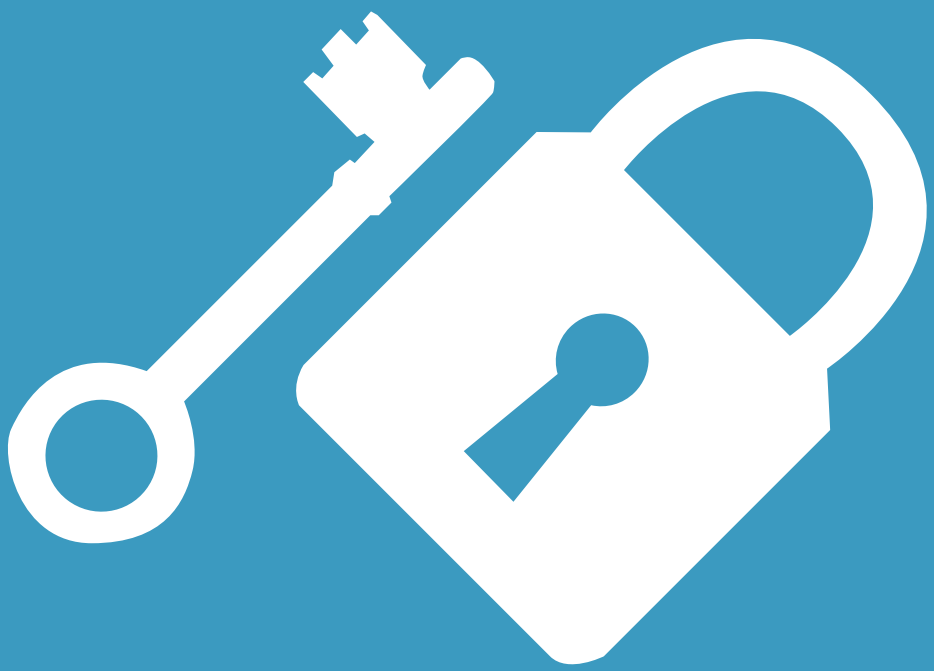
Cognizant
Passion for making a difference

Associate Security Handbook

Version 1.0



Issued by
Satish Das, Chief Security Officer
Chandrashekaran Krishnaswamy (KC), Head – Administration and Network and System Services

For internal circulation only.
Not to be distributed outside Cognizant

Contents

1. Why have you been given this handbook ?

Everyone in Cognizant has a role to play in ensuring that the company remains secure. This guide has been prepared to help you understand your responsibilities with regard to security in Cognizant. It will also give you some insight into the reasons for implementing different security controls and the procedures to be followed for raising security incidents or requesting security exceptions. Most importantly, it will prevent you from getting in trouble by unintentionally breaching a security policy. Please note that this handbook is a supplement and not a replacement for other security awareness programs or security policies.

Complete reference of Cognizant security policies can be found at:
Intranet: https://conline/qview/corporate/information.html under information security section
Internet: https://conline.cognizant.com/qview/corporate/information.html under information security section

2. Security Facets

Security has three facets:

- **Information Security** refers to safeguarding information from unauthorised access, manipulation and misuse, and ensuring that information is available to the right person when required for business purposes.

- **Personnel Security** refers to the procedures established to ensure that all personnel with access to sensitive information, have the required authority and the appropriate clearances.

- **Physical Security** is responsible for ensuring safety of Cognizant's associates, as well as protection of the company's physical resources from unauthorized access, damage or destruction.

3. Importance of security

Maintaining security is critical to our company. A security breach can result in:

- Damage to Cognizant's reputation
- Disruption of work
- Law suits
- Regulatory penalties
- Embarrassment to customers, associates and management
- Damage to Cognizant and/or Customer assets

4. Your Responsibilities

4.1. At the time of induction / joining Cognizant

Awareness is the key to ensuring the company's security as well preventing accidental security violations. Please ensure you complete the following mandatory security awareness programs when you join:

- The Acceptable Use Policy (AUP) e-Learning program.
  This program covers what constitutes acceptable use of Cognizant resources and is available at:
  Intranet: http://myacademy/elearning/ | Acceptable Use Policy | Acceptable Use Policy eLearning
  Internet: http://myacademy.cognizant.com/elearning/
  | Acceptable Use Policy | Acceptable Use Policy eLearning

- The Code of Business Ethics (COBE)
  This program covers ethical conduct within Cognizant and is available at:
  Intranet: http://myacademy/elearning/
  Internet: http://myacademy.cognizant.com/elearning/

- Induction sessions
  Various teams such as the Global Information Security (GIS), the Network & Systems Services (NSS), Administration and Human Resources will take you through some of the security policies and processes, during your induction.

- Read and understand the non-disclosure agreement (NDA) carefully before you sign it.
  The Cognizant's NDA requires that you do not share details of your work even after you leave Cognizant.

4.2. At the time of joining a project

When you join a project, please ensure you:

- Obtain new login credentials from the Client (through your Manager).

- Do not use the login credentials of any one else in your project, or someone who has left the project, unless explicitly authorized by the Client. If you are forced to use someone else's login credentials without proper authorization, please report it directly to the Chief Security Officer (CSO).

- Familiarize yourself with the Client's security policies & security requirements as you will now have to comply with both the Client's and Cognizant's security policies.

- Familiarize yourself with the Incident Reporting process.

- Acquaint yourself with the project Business Continuity Plan (BCP - refer Glossary) process.

4.3. When travelling onsite

If you are deputed onsite for your project please ensure that you:

- Honestly and thoroughly complete all immigration related forms and plan your travel only after consulting with the Global Immigration Team (GIT).
- Have proper documents to work at the client location.
- Check the latest security updates sent out by the CSO or the GIS team.
- Always carry your passport and tickets with you. These are critical documents and it is recommended that you keep them on your person and not in carry-on baggage.
- If you are carrying a laptop, always use the laptop lock to prevent theft.
- Always keep an eye on your baggage especially while exiting the airport or at currency exchange counters.
- Inform the GIS team immediately in the event your laptop is stolen (refer to sections on laptop security).
- Associates in the possession of portable, laptop, notebook, palmtop, PDAs, Blackberry and other transportable systems containing confidential information must not check these in airline luggage systems. To avoid damage and theft, these systems must remain in the possession of the traveler as hand luggage.
- Confidential information must not be read, discussed, or otherwise exposed in restaurants, on airplanes/ trains, or in other public places.

4.4. During the project

When in a project there are certain important guidelines that need to be followed. Please ensure that you:

- **Do not share your Client-provided password or log-in credentials with anyone.**
- **Do not use any freeware, trial or evaluation software in your project deliverables.**
- Inform your Manager and the GIS team immediately if you lose any Client provided asset such as a secure token.
- Do not share your work details even with Cognizant associates outside of your project without

prior approval from the Client. In case of any doubts, please contact your Manager for assistance.

- Ensure confidentiality of all work transacted while executing a project.
- Do not send codes, large files, and project critical documents to customers as e-mail attachments. Please use the SFTP facility. Unencrypted email is not a secure mode of transferring important material.
- Do not copy sensitive project documents onto removable media like USB storage devices, CD/DVDs, etc.
- Raise a request on the GIS portal if a DVD/ CD back-up is required for business reasons
  Intranet: https://gis
  Internet: https://gis.cognizant.com
- Do not share the source code with anyone outside your project. Any document you develop automatically becomes the sole property of Cognizant or the customer for whom it was developed.
- Label your work as C1, C2 or C3 (refer glossary), as appropriate. This classification ensures that the assets you have created or are working on, are adequately protected. Please read the Information Labeling and Handling Guidelines for any clarifications at links provided in Section 1.
- Do not leave hard/soft copies of any document labeled C1/C2 critical (e.g. design specifications, source code, RFPs) in common places like conference rooms and printer locations. In case you find one, please bring it to the notice of the associate who sent the print (their ID would be printed at the top-left corner). Shred them if you are unable to locate its owner.
- Clear your desk of any unused papers or objects lying around. Refer to the periodic clear-desk policy e-mails sent by your local administration team.
- Please do not bring any electronic material such as floppy disk/CD/DVD/USB storage devices etc into Cognizant. However, if there is a pressing business need to do so, please ensure that you have your Manager's and the GIS team's approval.
- Print the minimum required. This conserves paper which in turn saves trees. It also decreases possibility of classified documents being leaked.
- Never print/ share anything which could be construed as indecent, obscene or hurt a fellow Associates' feeling.
- Working from home or alternative site work arrangements (telecommuting) is a management option, not a universal fringe benefit. Permission to telecommute has to be approved by the involved associate's manager and GIS.

4.5. Project Email Usage

When communicating through emails please ensure that you:

- Do not email sensitive non-public information (Client's customer information such as name, address, telephone numbers, SSN(refer glossary), passport no, Tax ID) to anyone (not even within your own project). Also never use customer issued IDs to email sensitive information to anyone outside the customer domain (such as sending sensitive project information from your customer ID to a Cognizant ID).
- Never use your personal (non-Cognizant) email IDs for project related communication.
- Never use auto-forward to/from your customer ID.

4.6. Client Provided Laptop Usage

The client security team must approve any use of customer-provided laptops in writing. This approval/no-objection certificate must contain the serial number and make of the laptop. Please keep in mind the following before bringing the laptop into Cognizant premises. You will need to:

- Obtain an approval from your Manager and the GIS team for using the laptop.
- Declare the laptop and its serial number at the main gate.
- Have the NSS team scan the laptop for latest anti-virus and patch updates, before connecting it to our network.

In case you need to use the laptop for more than a week, please ensure you:

- Get a temporary laptop pass issued by the location Admin team.
- Get the laptop scanned by the NSS on a weekly basis .
- Avoid accessing internet from home using the customer laptop, as your broadband / dialup connection may not have the necessary security controls to keep hackers at bay.
- Do not install any Cognizant Licensed Software on the Laptop.
- Always use a laptop lock to physically secure your laptop to a work area. If you don't have a laptop lock, please contact your local NSS team, or a Client contact, for assistance.

Associates are expected to adhere to client's security policy while using client provided laptops.

4.7. At the time of leaving a project

When you leave a project, please ensure you:

- Return any secure token or other Client artifact you may have received during the project to your Project Manager.
- Request NSS to sanitize your desktop/ laptop to delete any project related critical information.
- Delete Project-related documents from your email inbox.
- Request your Manager to -
  - Inform the Client that you are leaving the project.
  - Have your access to project resources (such as server shares, email distribution lists, knowledge repositories etc) deactivated.
  - Modify the project BCP if you held any BCP responsibilities.

4.8. While working in Cognizant

While working in Cognizant it is important that you are aware of the latest security guidelines and that you adhere by them.

4.8.1. Continuing Security Awareness Programs

Ongoing security awareness programs include:

- Reminder emails sent out by Admin, NSS, GIS or other groups to reinforce key security policies or for emergency situations.
- Security posters.

Please take all security related communications seriously—as violations are considered severe and can lead to the extent of terminations.

4.8.2. Using company provided systems

All Cognizant systems are meant for business use only. Downloading unauthorized software or other unacceptable material might result in damage to company assets and might even render the company liable to lawsuits. To put it simply, please refrain from downloading, storing or using MP3 files, pornographic materials, pirated software, software without valid licenses etc. The AUP training will take you through the acceptable use of company resources. Please be aware that Cognizant follows a zero tolerance policy in such issues.

4.8.3. Desktop/Laptop Usage

Following are the desktop/laptop usage guidelines:

- Make sure that any special privileges on your desktop (e.g. Administrator rights, CD/DVD/USB enabled, IIS installations) are backed up by the relevant approval from your Project Manager and the GIS team (if required).

- In case you have Administrator rights over your desktop, please ensure that you do not disable the preconfigured settings such as password-protected screensavers, anti-virus agent etc. Any attempt to do so constitutes a serious security violation and shall invite disciplinary action.

- Do not forget to lock or log off your system/account when you leave your desk unattended. Please ensure that the local anti-virus agent is always running in your desktop. Click the Virus Scan Icon and select the "About" Option to know more.

- Anti-virus signatures are updated almost daily. In case the anti-virus update is older than three days, log a ticket in GSD Helpdesk.

- Do not store media files like MP3, WAV, video clippings and profane images on your desktop/laptop or server shares. In case there is a genuine business requirement to store media files, they must be communicated to the GIS team.

- If you notice any system-related suspicious activities, first log them to the GSD Helpdesk and then inform the GIS team for immediate action.

- Any usage of Cognizant provided laptops must adhere to the company's security policy at all times.

- Your desktop is subject to periodic audits by the security team – protecting it and ensuring that it adheres to the security policy is your responsibility.

4.8.4. User IDs and Passwords

User id and password is very sensitive information. It is extremely important that you:

- Never share your password. You are responsible for all transactions undertaken with your user ID and password.

- Choose a sufficiently complex password that would be hard to crack.

Apart from selecting a secure password, also remember a few best practices related to password protection:

- Never disclose your passwords to someone else.
- Never write passwords anywhere.
- Do not chose words related to you (such as your name, date of birth or spouse's name) as passwords.
- Do not use common words or those that appear in the dictionary as passwords.
- Change your password if you suspect someone knows of it.
- Beware of phishing (refer glossary) and social engineering attacks – the GSD or NSS staff would never ask you for your password.
- You can use Cognizant's Identity Management system to change and manage your network password. Please refer to the section on 'How to Manage Password' under Cognizant Identity Management System – Quick Tour (on the login page)
  Intranet: https://identity/enrole
  Internet: https://identity.cognizant.com/enrole

4.8.5. Using Cognizant Email

Please remember the following while using the email facility provided by Cognizant:

- Email conversations should not be considered private. Cognizant reserves the right to audit/block your emails with sensitive content.
- Do not forward/propagate any chain mails or emails containing jokes, stories, and pictures.
- Be careful while opening email attachments received from unknown senders – these are likely sources of viruses and other malicious codes which could harm your system.
- Do not transfer any software or copyrighted material using emails unless the recipient is authorized by the copyright holder to store and use that material.
- Do not register your official email with newsgroups or public forums.
- Maintain proper etiquette and professionalism in all your email conversations – informal or otherwise. All emails are identified as originating from the company, which puts Cognizant's reputation at stake.

4.8.6. Dealing with Spam

- Never, ever reply to a spam (refer glossary) message: Spam subject lines usually promise you a better life, a more youthful appearance, love, thicker hair, or a better mortgage rate. Please don't open it. Report it and then delete it.

- Don’t click any links in a spam e-mail: This includes buying a product that is for sale or clicking the often-misunderstood “unsubscribe” link, which actually informs your spammer that you exist.

- Disguise your e-mail address: Don't put your e-mail address in plain text on any web site.

- Disguise your e-mail address by stripping out periods and "@" symbols as an image which will prevent spammers from identifying it.

- Don’t forward an e-mail from someone you don’t know to a list of people: You remember those “forward this e-mail to 20 of your friends” messages to get good luck, have cash deposited in your bank, help some worthy soul or for some equally ludicrous reason? They are perfect for spammers to harvest e-mail addresses.

- Don't use your regular Cognizant/Personnel email address when you register at Web sites.

- If you receive spam, please forward it as an attachment to reportspam@cognizant.com

4.8.7. Network & Internet Usage

Please keep these guidelines in mind when using Cognizant provided network or internet resources:

- Company provided internet/ network should not be used t o access/download/store/distribute pirated software, games videos, MP3s and other similar files.

- If you intend to use any freeware/shareware for evaluation or project purposes, please have it approved from your Manager and the GIS team. You must then register the software as a freeware with NSS and raise a RAMS request to have it installed in your system.

- Do not attempt to access any data/server/network-resource that you are not authorized to – such cases will be considered as security violations.

- Do not execute any form of network monitoring, port scanning or packet sniffing.

- Do not solicit/provide information or help on public forums and mailing lists unless there is a clear business need to do so.

- There can be no legitimate business reason to access any illegal, pornographic or other material with which the company would not wish to be associated. Any such activity is strctly forbidden and will invite disciplinary action.

4.8.8. ID and Access Cards

As long as you are within Cognizant premises, it is important that you:

- Wear and display your identity card. Your ID card should be visible to:
  - Ensure identification of unauthorized people who have managed to get past the main gate security.
  - Identify strangers in the work area.

Please also note:

- Your Cognizant ID card proves your association with Cognizant.
- Do not allow anyone else to use your ID or Access card.
- You need to be sensitive of anyone tailgating you. If you feel they are not part of Cognizant, please verify if they are visitors or vendors.
- If you forget your ID card, the Security at the front desk will issue you with a new card after authentication. You may be required to provide acceptable (Government or bank issued) photo ID such as a driving license, passport, photo credit card, or PAN card for identification – photocopies are not acceptable.

4.8.9. Viruses

All Cognizant desktops and laptops are updated automatically with the latest anti-virus patches. However, technical issues may result in the anti-virus not being updated on time. To protect your system, please ensure that you:

- Manually update the anti-virus on your system if it is more than 3 days old. You can do this by right clicking on the antivirus icon on your taskbar and clicking on “Update now” option. In case of further problems, contact your local NSS representative for assistance.

4.8.10. DVD/CD Back-up process

When backing up project resources:

- GIS recommends using SFTP or project shares for all file transfers. NSS-provided tape backups are recommended for all project-related backups.

- In case the business requirement still requires you to create a CD/DVD, please raise a request on the GIS Portal under 'CD/DVD Creation'.

- Please remember that you would be responsible for ensuring the security of the CD/DVD. You could be held liable for any loss of confidentiality that arises from the loss/theft of the CD.

- Please return the CD/DVD to NSS for destruction once the business requirement is over.

4.8.11. Handling Classified Documents

When handling classified documents ensure that you do not:

- Leave hard copies of any document labeled C1/C2 critical (e.g. design specifications, source code, RFPs) in common places such as conference rooms and printer locations. In case you find one, please bring it to the notice of the associate who gave the print (their ID would be printed at the top-left corner). Shred them if you are unable to locate its owner.

- Confidential documents should not be taken out of the building without approval.

- Whenever hardcopy version of confidential information is removed from Cognizant premises, it must either be stored in a safe or in a locked container. Such information must not be left in an unattended motor vehicle, hotel room, office, or some other publicly accessible location, even if the vehicle or room is locked.

4.8.12. Personal Laptops

We would like you to be informed of the fact that bringing personal laptops into Cognizant is prohibited, with no exceptions. Any personal laptops found in the premises are liable to be seized for investigation.

4.8.13. Photography

Taking pictures within sensitive areas (Data Centers, Project Areas etc) is prohibited. In case you need to take pictures in any other areas, please ensure that you have prior approval from your Manager and the GIS team.

4.8.14. Visitors

When inviting visitors to the facility please note the following:

- Personal (relatives and friends) are welcome to visit Cognizant facilities, but only till the facility reception area. Personal visitors are not allowed inside the rest of the facility. This category of visitors includes bank representatives or credit card salesmen.

- Business visitors to Cognizant facilities must be approved by a Manager (APM or above). They would need to be escorted at all times within the software development areas. These visitors may be asked to provide proof of identification (driving license, photo credit card, or passport) before admission.

4.8.15. Receiving personal snail mail/couriers at office

Receiving personal post/couriers at the Cognizant office is not recommended. While you can use a Cognizant facility as your mailing address, the company does not accept any responsibility for loss or misuse of your posts/ courier deliveries. Please be sure to update your address in case you change offices or leave the company.

4.8.16. Transport Security

Your safety is very important to us. If you ever feel unsafe while using company arranged transport, please contact the local Admin/ HR immediately.

4.8.17. Fire Drills

If a fire drill commences, please drop whatever you are doing no matter how important it is (coding, attending a client presentation, attending a teleconference) and follow evacuation procedures.

4.8.18. Emergency Situation

An emergency includes eventualities such as fire, floods, earthquakes, bomb threats etc. In such situations please do not panic when the alarms sound. The concerned department will investigate the matter and then instruct you (through the Public Address system, email or other medium) on the procedure to be followed (including evacuation of the facility). Also please read any security advisories sent out by the CSO before or during such calamities.

4.9. At the time of leaving Cognizant

You might be surprised to know that your security responsibilities do not end even as you pursue other opportunities. The non-disclosure agreement (NDA) you sign with the company is binding even after you leave!

4.10. Security Exceptions

Certain business requirements call for a relaxation of the security policy. For such exceptions the business justification along with a Project Manager's (note – for security approvals, an Assistant Manager's approval is not enough) approval is required. If your Manager is not available, then approval must be received from his/ her Manager. In some cases, approval from the Client or the Client's security team may also be required. The Cheat Sheet given on the last page will let you know where to raise exception requests.

4.11. How do I report security violations?

You can report any security incidents through Global Service Desk through:

- Intranet: https://gsd
  Internet: https://gsd.cognizant.com
  Voice Net: 56666
  Telephone (USA– Toll Free): 1-866-822-2024
  Telephone (USA): 973-368-9500
  Telephone (UK): 207136-1414
  Email: gsd@cognizant.com

- If you are worried about getting in to trouble by reporting a security breach, the GSD portal has a facility for reporting incidents anonymously (you do not have to disclose your name, employee ID or any other identification).

- You can also email the GIS team for serious security incidents. For something of critical importance, please contact the CSO directly at cso@cognizant.com.

- For a refresher on information systems security retake the Acceptable Use Policy course at:
  Intranet: http://myacademy/elearning
  Internet: http://myacademy.cognizant.com/elearning/

- Should you need more clarification, please contact the Chief Security Officer, directly

- The FAQ on security incidents is available at:
  Intranet: https://gis/TrainingEducation/Awareness/default.aspx
  Internet: https://gis.cognizant.com/TrainingEducation/Awareness/default.aspx

4.12. What are the consequences of violating security policies?

Non-compliance or violation of the security policy will result in action that may include:

- Suspension / Termination of employment

- Other disciplinary action

- Criminal prosecution

Please take Cognizant's security policies seriously.

5. Glossary and Abbreviations

Anti-virus

Software designed to detect, and potentially eliminate, viruses before they have had a chance to wreak havoc within the system, as well as repairing or quarantining files are infected.

BCP

A Business Continuity Plan is a comprehensive written plan to maintain or resume business in the event of a disruption. (Such as a server crashes, fire, floods).

Cracker

Refers to either a computer program whose purpose is to 'crack' the code to a password or a person who attempts to gain unauthorized access to a computer system (a malicious hacker).

CCO

Chief Compliance Officer

CSO

Chief Security Officer

CRO

Chief Risk Officer

Encryption

The process by which data is temporarily rearranged into an unreadable or unintelligible form to maintain confidentiality, for transmission, or other security purposes.

Firewall

Firewalls are security devices used to restrict access in communication networks. They prevent computer access between networks (say from the Internet to your corporate network), and only allow access to services which are expressly registered.

GIS

Global Information Security team

GIT

Global Immigration Team

GSD

Global Service Desk

Hacker

An individual whose primary aim is to penetrate the security defences of large, sophisticated, computer systems. Hackers are a threat to all computer systems that allow access from outside the organization's premises. The fact that most 'Hacking' is just an intellectual challenge should

not allow it to be dismissed as a prank. Clumsy hacking can do extensive damage to systems even when such damage was not intentional.

Information & Asset Classification

C1 – Highly Critical
C2 – Critical
C3 – Protected
C4 - General

ITRMG

Information Technology Resource Management Group

NPI

Non Public Information

NSS

Network & Systems Services

PII

Personally Identifiable Information

PIFI

Personally Identifiable Financial Information

Phishing

A criminal activity using social engineering techniques. Typically, criminals attempt to acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication. The fake messages generally include a link to phoney websites, where victims are asked to provide sensitive, personal information. The information goes to criminals, rather than the legitimate business. Such attacks can also take place using SMS or voice calls.

PIHI / PHI

Personally Identifiable Health Information / Protected Health Information

Privacy

For details of PII, PHI, SI please refer Cognizant's Privacy Policy at:
Intranet: https://conline/qview/corporate/Information.html
Internet: https://conline.cognizant.com/qview/corporate/Information.html

RAMS

Resource Allocation and Management System

SFTP

Secure FTP. A secure way to transfer files between different locations

SI
Sensitive Information

Social Engineering
It is the collection of techniques used to manipulate people into performing actions or divulging confidential information.

Spam
Spam refers to unsolicited e-mail usually sent with a malicious motive. Computer Spam is the electronic equivalent of Junk Mail.

Trojan
A Trojan is a virus that is disguised as something benign, such as a desktop search tool, an archiving program, or a game. A Trojan normally requires a user to perform some action before the virus can be activated.

Virus
The term Virus includes all sorts of variations on a theme, including the nastier variants of macroviruses, Trojans, and Worms, but, for convenience, all such programs are classed simply as 'virus'. A virus is a form of malicious code, which may be transferred unknowingly from one computer to another. A virus can create disruptions such as slowing down the computer, deleting data, or causing the system to crash.

Worm
Worms are classified as a type of virus. A Worm is a program that propagates itself over a network, reproducing itself as it goes. The term has acquired negative connotations, as it is assumed that only crackers write worms.

Notice
Some policies or procedures might be changed from time to time to stay current with emerging threats – please keep yourself updated from GIS.

Cheat Sheet (Reference Guide)

GIS is not the only group with security responsibilities. Here is a summary of the security related tasks performed by groups within Cognizant. You can reach out to these teams for:

Reporting security incidents – Global Service Desk (refer section on reporting security violations).

Reporting virus on your computer – Global Service Desk.

Reporting spam – Messaging Team at reportspam@cognizant.com

Firewall enablement – raise a request with NSS at -
Intranet: https://firewall | Internet: https://firewall.cognizant.com

Forgot ID card at home – Security at Front Desk. Reception will issue you with a new card after authentication.

Permanently Lost/ misplaced ID/ Access Card – local Administration team.

Fire alarm/ smoke detector malfunctioning – local Administration team.

Theft of personal property in the office premises – local Administration team.

Requesting software – Intranet: https://rams | Internet: https://rams.cognizant.com

Software not available at RAMS – Intranet: https://gis | Internet: https://gis.cognizant.com

Burning a CD/DVD – Intranet: https://gis | Internet: https://gis.cognizant.com

Requesting access to a blocked website – Intranet: https://gis | Internet: https://gis.cognizant.com

Unethical practices within the company – Chief Compliance Officer.

For any other serious issues contact the Chief Security Officer at cso@cognizant.com

Any other security exception – contact the Global Information Security team at gisteam@cognizant.com

Cognizant
Passion for making a difference

Cognizant
Passion for making a difference