Project Manager Security

Handbook 2.0

Released by

Satish Das

Chief Security Officer

Project Manager SECURITY

This handbook helps you protect Cognizant by securing your project. It provides an overview of your security responsibilities and guidelines for security best practices. For details, refer to Cognizant security, business continuity and privacy policies link provided in the Cheat Sheet.

Please note that information security is very dynamic and new threats are continuously evolving. As such some of the controls mentioned in this Handbook may be modified without notice in the interests of the organization's security. Please touch base with GIS team for any assistance.

Contents

1. Why are you responsible?

As a Manager you would be required to make five kinds of security decisions:

1. Approving – Verifying resource / access / other requests from your team and approving them if they are justified from a business standpoint.
2. Rejecting – Not granting requests which are not justified from a business standpoint.
3. Escalating – There will be some decisions which you will not be able to take a call on. In such cases you will need to escalate the issue to Senior Management or to GIS team.
4. Reporting – Any security incidents within your project should be reported to the security team for investigation.
5. Compliance – Ensuring your project complies with the security requirements of the Client Master Service Agreement or Cognizant Security Policies.

Read on to understand when you will be required to take security decisions…

2. Project Start

At the start of your project, check for the following:

2.0.1 Familiarise yourself with the security terms of the Client MSA.
2.0.2 Ensure that the project Quality Auditor is also aware of the security terms of the MSA so that the project can be audited for the same.
2.0.3 Ensure that the project has a BCP in place (for details refer to the Business Continuity Planning section).
2.0.4 If the project has access to confidential personal information or other sensitive data, please check the possibility of using data masking or sanitising tools.
2.0.5 Refer to the section on Restricted Access if your project is physically isolated.
2.0.6 Ensure all Associates in the project have completed required Client and Cognizant security awareness programs (refer section on Security Awareness).
2.0.7 Ensure background verification has been completed for all Associates joining the project (refer to the section on Background Checks). Please contact your Talent Manager for help with this.
2.0.8 Ensure that Client supplied software has been updated in RAMS – contact ITRMG group for any assistance.
2.0.9 Ensure Client NDA has been signed.

2.0.10 Brief project members to take care of Client provided resources.

2.1 Background Checks for your Project's Associates

Cognizant's Personnel Security Policy requires background checks to be completed for all Associates. Especially for lateral hires, please check with your Talent Manager that the Associate's background check has been completed before allowing him / her access to critical resources. Please ensure that all campus recruits in your project have applied for passports so that their backgrounds will also be checked. A negative background check report will result in termination of the Associate, regardless of his / her criticality to the project.

2.2 Data Protection

2.2.1 Label all project artifacts C1, C2, C3 or C4 based on their confidentiality, integrity and availability ratings for details refer to the Information Labelling and Handling Procedures at: https://c20ecosystem/Process%20Space/default.aspx

2.2.2 Ensure that critical artifacts are not stored on desktops or laptops. These systems have weaker access controls and if they crash, the data cannot be recovered. Please store such artifacts in servers only and request NSS to take back-ups.

2.2.3 Review access to project shares and other project resources on a monthly basis.

2.3 Business Continuity Planning (BCP)

In case business disruptions occur, your project will need a Business Continuity Plan to be able to sustain Client deliverables:

2.3.1 Your project needs to have a BCP documented within 30 days of project start date. BCP Coordinators can also take up the BCP training available on the BCP portal (https://bcp or https://bcp.cognizant.com).

2.3.2 The BCP Coordinators identified by you can create the project BCP in the BCP portal after which the plan will be sent to you for approval.

2.3.3 Once the plan has been created and signed-off by the Client, you may contact the BCP Helpdesk to have it tested.

It is the Project Manager's responsibility to ensure Client mandated BCP

requirements are met.

3. During the Project

3.1 Project asset inventory management

Clients may have provided your project with assets such as security tokens. Please maintain an inventory of such assets to ensure they are not misplaced. Inform GIS team immediately in case of theft or loss of such assets.

3.2 Offshore Development Centers (physically isolated projects)

If your project is physically isolated, please review the list of personnel who have access to the project area on a monthly basis. If you are not receiving a monthly access report, please get in touch with your local Admin dept and ensure you receive the report.

Inform all Associates in your project that any non-business visitors (even other Associates who are not part of the project) should be met outside the project area.

If a project member reports to work without his access card, the physical security or Admin team may call you to verify the Associate's identity. If possible, please notify the Admin team in advance if any of your project members need to work on weekends or holidays.

3.3 Privacy

Privacy is a major concern for all our Associates, Clients and their customers. Privacy is an overarching concept and goes beyond just establishing confidentiality requirements. Your responsibilities regarding privacy are as follows:

3.3.1 Understand that the Cognizant Privacy Policy covers Clients, their Customers and Associates' Personal Information.

3.3.2 Check whether your project has access to Personally Identifiable Information (PII). This could be financial information relating to individuals (such as Credit Card or SSN numbers) or general information regarding addresses, telephone numbers and so on.

3.3.3 If your project does have access to any kind of PII, it is your responsibility to inform all project members not to discuss such information, even within the project team. Such information should not be stored in project

desktops, written or circulated anywhere.

3.3.4 Recheck your MSA and ensure that you have incorporated all the security measures required to safeguard PII.

3.3.5 Even if your project does not have access to PII, please ensure that your team members' personal information is not shared outside Cognizant (even to Clients).

3.3.6 For more information regarding privacy, please read the Cognizant Privacy Policy or contact the Chief Security Officer. For privacy related training, please refer the Security Awareness Training Section (7.1)

3.4 BCP review

Please ensure the project BCP is reviewed and updated in the BCP portal in case of any changes in project location, set-up, project call tree etc.

3.5 BCP Situations

BCP situations may arise due to both natural (floods, torrential rains, earthquakes) or man-made (network failure, fire, riots) reasons. In such cases, please contact the BCP Helpdesk.

3.6 Account Security Risk Assessment (ASRA)

Cognizant has a strong culture of risk management. To ensure project security risks are identified and mitigation measures documented, your project's PMO must complete the Account Security Risk Assessment at https://asra on an annual basis.

3.7 Onsite Travel by Associates

3.7.1 Ask Associate to read the travel advisories issued by the Chief Security Officer.

3.7.2 Ask Associate to submit any CD / DVD requests well ahead of the travel date. This is to ensure that there is enough time to approve and burn the CD / DVD – refer to the section on CD / DVD Back-ups for details. Associate has to ensure back up data is password protected.

3.7.3 Have the Associate return his / her access card to Admin if the travel is for a period greater than 2 months.

3.7.4 If the Associate is carrying a laptop, ensure he has laptop lock issued by NSS.

3.7.5 Instruct Associate to raise a GSD ticket to inform GIS immediately if laptop

or DVD is lost or stolen.

3.7.6 Educate the Associate to read the Client security requirements while he / she is in the Client location.

3.8 Security Incident Handling

If your project gets involved in a security incident, there is no need to panic. Please note the following:

3.8.1 Do's:

- Immediately report the security incident in the GSD system. (Refer to the Cheat Sheet for how to report security incidents.)
- Review the Client MSA to understand possible implications / penalties of the incident.
- If any sensitive information or data leakage is suspected, please contact the Legal team as well as GIS.

After the incident has been reported, the GIS team shall advise you on any immediate steps required to contain the incident. GIS will then conduct an investigation and provide a detailed Investigation Report which can be shared with the Client.

3.8.2 Don'ts:

- Do not send any ethical or HR related incidents to the GIS team – such incidents should be forwarded to the Chief Compliance Officer or local HR as the case may be.
- Do not over-commit to Clients regarding dates by which the investigation shall be completed or actions which shall be taken. The GIS team shall provide relevant dates after preliminary discussions with the project to understand background of the incident. The corrective actions will also be finalized after the investigation is complete.

3.9 Creation & Management of Third Party / Client / Contractor IDs

Emails are an ineffective and dangerous way of granting, managing and revoking user accounts. Cognizant uses the Tivoli Identity Management (TIM) system to automate this work-flow and ensures that we provide the user accounts to right people and revoke them at the right time.

Use the Identity Management System https://identity/itim/self (intranet) or https://identity.cognizant.com/itim/self (internet) for user provisioning / de-provisioning for all non-Cognizant resources. You have to use the system to create, renew or delete any 3rd Party, Client or Contractor User IDs.

For queries regarding TIM usage, please contact the Global Service Desk https://gsd or vnet 56666.

3.10 Project Movement

If your project is changing locations please ensure the following:

3.10.1 Check your MSA whether Client sign-off is required before moving to a new location.
3.10.2 Make sure that local NSS has sanitised the hard disks used by your project so that any new users of project PCs do not gain access to data inadvertently left behind.
3.10.3 Update your BCP with changes of location, contact persons etc.
3.10.4 Ensure new location has the level of security required by the Client MSA.
3.10.5 Ensure access to project shares has the same level of restriction (in case project material is being moved from existing servers).

3.11 Project Laptops / Mobile Devices

Please note the following for project laptop usage:

3.11.1 Ensure laptop usage for project deliverables is allowed by the Client.
3.11.2 Confidential Client information like SSNs, credit card numbers, Personal Information etc. should never be stored on laptops or mobile devices.
3.11.3 If confidential Cognizant information is stored on a laptop, please ensure it is encrypted and has a Data Leakage Prevention (DLP) agent installed (contact local NSS team for assistance with this).
3.11.4 Laptops should always be secured using a cable lock when unattended.
3.11.5 Instruct project members to check that the anti-virus is updated. If it is outdated, this should be done manually.

3.12 Client Supplied Laptops

For Client provided laptops which are going to be used in Cognizant facilities:

3.12.1 Send an approval letter / email from Client with laptop details (model / serial no.) and person / period of allocation to GISHelpDesk@cognizant.com.

3.12.2 Have NSS check the laptop for latest Anti-virus / Patch Definitions (no Client provided software should be un-installed, also no Cognizant licensed Software to be installed on the laptop).
3.12.3 If the Client has an isolated ODC then the laptop can be connected to the network. Else, the laptop needs to be logically segregated from Cognizant network using appropriate access-list restrictions.
3.12.4 Ask NSS to provide access only to the identified VPN / remote Server IP address and block all other access to the network.
3.12.5 Provide the details of how the laptop would be updated with Anti-virus signatures / Patch updates to NSS - please note this would not be taken care by local NSS team, hence you need to make sure the laptop is updated periodically with the latest security updates.
3.12.6 Collect a temporary laptop pass from NSS for the stated period.
3.12.7 Connect the laptop to the port identified by NSS only.

3.13 Transferring files between onsite / offshore

3.13.1 Ensure Project artifacts are shared between onsite and offshore through Client approved means.
3.13.2 As far as possible use secure means of file transfer -SFTP,HTTPS etc.
3.13.3 Use Client or Cognizant dedicated SFTP Server for secure file transfer – you may raise a request in https://gsd for Cognizant SFTP related requirements.
3.13.4 If the Client insists on using a third-party social publishing site, please request written confirmation from the customer security team.Example: Google Docs, DocStoc.com
3.13.5 Please avoid transfer of files using unencrypted removable media like USB drives, portables hard disks etc. If the portable media is encrypted, then the decryption key should be shared separately over a different communication channel. Usage of personal devices to transfer Cognizant or Client data is not allowed

3.14 SSAE 16 / ISAE 3402 / SAS 70 / PCI / Client Security Audits

Clients may require your project to be audited for security. These audits may be conducted by the Client or designated representatives. Projects may also be required to have themselves audited for SAS 70 or Payment Card Industry (PCI) compliance. To ensure that such audits are effectively and efficiently managed, please get in touch with the center's GIS coordinator who will guide you regarding audit preparations.

4. Associates leaving your project

4.1 Normal Exit

If an Associate is leaving your project please ensure that the following is completed within 24 hours:

4.1.1 Remove his access to all project resources (project server shares, Knowledge Repositories (KRs), email Distribution Lists (DLs) etc.).
4.1.2 Recover any Client provided Secure Tokens or Access Cards. If you cannot recover, notify Client to deactivate immediately.
4.1.3 Inform the Client that the Associate has left the project.
4.1.4 If possible, reset all passwords the Associate had access to.
4.1.5 If your project is located in a physically restricted area, ensure that his / her access to the project area is withdrawn.
4.1.6 If the Associate requests a CD back-up of personal information, refer to the CD / DVD back-up section.
4.1.7 Debriefing session – inform the Associate that:

- He / she is still bound by the NDA signed even after leaving the project.
- All project related materials (including emails) should be copied to the Project Share.
- All personal information should be removed from his/ her workstation or laptop.

4.2 Absconding / Terminated Associate

Inform Admin and HR to revoke all accesses immediately & inform Client as required. Report to HR if an Associate has not reported to work / established contact for 3 days without prior approval.

5. Security Exceptions

At times you may have to request security exceptions for your project. Please note the following:

1. Please provide business justification whenever raising exception requests.
2. Some exceptions may require approval from Client security or business teams. Such approvals may be required because there are security commitments made to Clients at an organization level which a project manager may not be aware of.
3. Please keep a record of any security exceptions granted to the project. This

may be required as evidence in audits.
Refer to the Cheat Sheet for details on how to raise security exceptions.

5.1 Allowing Local Admin Rights

For use of special software, an Associate may require Local Admin Rights to his PC. Please verify whether the Associate really requires these rights. Admin privileges can be easily misused to circumvent security controls or install unauthorized software including P2P software, Instant Messengers and computer games. Such software can result in data leaks (intentional or unintentional), IP violations and / or non-compliance with Client MSA.

5.2 CD / DVD Back-ups

Allowing back-up of data to a CD / DVD leads to immediate loss of confidentiality once the CD / DVD moves out of Cognizant premises. Note the following:

5.2.1 Check whether the Client MSA allows a CD / DVD back-up (many MSAs strictly prohibit this).
5.2.2 Check for alternate secure methods of transferring the data (eg through project shares or secure FTP).
5.2.3 It is the Project Manager's responsibility to verify that confidential data is not burned on any CD / DVD. Any loss of confidential Cognizant or Client data because of CD / DVD misplacement shall also be the Project Manager's Responsibility.
5.2.4 CD / DVD burning requests for Associates leaving Cognizant should not be entertained under any circumstances.
5.2.5 An Associate leaving the project shall only be allowed to take a back-up of his pst file. No other data shall be allowed to be transferred.
5.2.6 If you still believe that a CD / DVD back-up is required, please ask the Associate to raise a CD / DVD burning request in the GIS portal.

5.3 Clients working in Cognizant

For Clients working in (not visiting) Cognizant facilities:

5.3.1 Ensure Client has a valid proof of ID so that temporary ID card canbe issued quickly
5.3.2 Refer to the section on Client Supplied Laptop to ensure the process is followed.
5.3.3 Temporary Access Card with restricted access to public areas and

specific project bay can be issued only if the stay period is more than 15 days.

5.3.4 Have Client escorted during his stay.

5.3.5 It is your responsibility to collect issued passes / cards once Client leaves.

5.4 Client or Guest Laptops

The Cognizant Security Policy prohibits allowing Client, Guest or Vendor Laptops to be connected to the Cognizant network. If an exception is required, please send an email to GIShelpdesk@cognizant.com. Note – if business visitor is not going to connect to the network, GIS approval is not required for allowing their laptops inside Cognizant premises.

5.5 Personal Laptops

5.5.1 Personal laptops are NOT allowed in Cognizant premises.

5.5.2 Exceptions shall only be allowed by the Chief Security Officer.

5.5.3 Admin shall seize any personal laptops found in Cognizant premises.

Kindly do NOT raise requests to allow any Associate in your project to bring in a personal laptop – such requests shall not be entertained.

6. Project Closure

Once a project has ended, check for the following:

6.1 Make sure that local NSS has sanitised the hard disks / servers used by your project so that any new users of project resources do not gain access to data inadvertently left behind.

6.2 Check and comply with your Client MSA for data archiving and terms for handing over project artifacts such as data, documents, KRs etc to the Client.

6.3 Return Client provided systems and secure tokens.

6.4 Inform NSS to delete all project-related email Distribution Lists.

7. Others

7.1 Security Awareness Training

Cognizant has several security training and awareness programs to help Associates and Managers understand their responsibilities. The primary training program for

managers / project leads is:

- Security & BCP for Managers (for anyone leading / managing a project)

In addition, please ensure that all Associates in your project (yourself included) have completed the following mandatory programs for all Associates (including Managers):

- Acceptable Use Policy (annual recertification required)
- Understanding Privacy (Project) – mandatory for all Associates accessing Personal Information (refer Section 3.3 on Privacy)

Finally, for Associates involved in coding activities, the following program is available:

- Secure Coding Practices

These eLearning programs are available at:
https://compass.learning.cognizant.com

Training compliance levels for your project are available at the below mentioned link (updated fortnightly):
https://channelone/sites/SW09/AcademyLearningReports/Shared%20Documents/Forms/AllItems.aspx

7.2 RFI / RFPs

RFI / RFPs may require inputs on security / BCP. Please email such requirements to GISRFPRespondents@cognizant.com. Please note that extensive security questionnaires require time to answer so kindly send the same as early as possible. Most responses will typically be provided within 3 days while some may take longer based on size.

7.3 MSA Reviews

To receive assistance in reviewing security sections of MSAs, please email: GISMSASupport@cognizant.com. Please ensure that all MSAs are reviewed by the Legal Team before sending to GIS.

Cheat Sheet: Important Resources

Sl	Area	Resource
1	Cognizant Security, BCP and Privacy policies	https://c20ecosystem/Process%20Space/default.aspx
2	Real time updates / assistance during a crisis (medical emergencies, accidents,civil disturbances, flooding etc.)	Call 24x7 Emergency Contact Center (ECC) at: 1800-200-2345 Email: ECC@cognizant.com
3	Responding to RFIs / RFPs / Due Diligence questionnaires	GISRFPRespondents@cognizant.com
4	Reviewing MSAs	GISMSASupport@cognizant.com
5	Requesting software (including freeware / shareware / trial software)	Intranet link: https://rams Internet link: https://rams.cognizant.com
6	Security Exceptions	Raise exception at GIS portal: https://gis (intranet) https://gis.cognizant.com (internet) or email to: gishelpdesk@cognizant.com
7	To create project BCP	Cognizant BCP Portal: https://bcp or https://bcp.cognizant.com
8	Assistance with BCP	bcphelpdesk@cognizant.com
9	Security / BCP awareness programs	https://compass.learning.cognizant.com
10	For all other security related queries	gisteam@cognizant.com
11	Chief Security Officer	CSO@cognizant.com

Security Incident Reporting

Sl	Issue	Contact
1	Ethical issues	Compliance Helpline at: https://www.compliancehelpline.com/welcomepagecognizant.com/
2	Spam	Forward the spam as an attachment to reportspam@cognizant.com
3	Information leakage, laptop theft, viruses, worms, trojans, spyware, anti-virus signature, patch updates or physical security incidents.	Log a call in GSD under the "Global Information Security" tab at: 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 You can also raise anonymous incidents in GSD. If it is a really sensitive issue, please email the Chief Security Officer at: CSO@cognizant.com
4	Epidemic like Dengue, Bird Flu, Chikungunya etc.	Inform local HR and contact the Emergency Contact Centre (ECC) at: 1800-200-2345
5	Theft of personal property in Cognizant (mobile phone, credit card , wallet etc.)	Cognizant is not responsible for loss of personal property in office premises but you can contact local Admin for help.