COGNIZANT'S

ACCEPTABLE USE POLICY

DOCUMENT LEVEL – LII

Cognizant Corporate Security

Author(s)				
Name	**EmployeeID**	**Designation**	**Vertical**	**Date and Time**
Chakraborty, Abhijit	121514	Director - Projects	Corporate Security	19/Jan/2017 12:47:35 (IST) +5:30

Reviewer(s)					
Name	**EmployeeID**	**Designation**	**Vertical**	**Date and Time**	**Remark**
Naftzger, Darren D	585525	Senior Director-CS	Corporate Security	19/Jan/2017 19:23:47 (IST) +5:30	Reviewed

Approver(s)					
Name	**EmployeeID**	**Designation**	**Vertical**	**Date and Time**	**Remark**
Shiembob, Henry W.	390335	Chief Security Officer	Corporate Security	21/Jan/2017 03:12:02 (IST) +5:30	Approved

Dear Associate,

Cognizant is committed to creating a secure and reliable work environment for our Associates and clients to achieve our common business objectives through innovation, collaboration and secure communication. Appropriate usage of Cognizant's and Cognizant's clients' information technology resources is critical to ensure compliance with our legal and contractual obligations, to protect and safeguard the confidentiality and integrity of our information and ensure the availability of our supporting information technology.

As Cognizant has continued to grow, our risk and regulatory landscape has changed and our clients' expectations and requirements have evolved, our Acceptable Use Policy (AUP) has been updated to address these changes. The AUP sets forth the Cognizant mandates with respect to the acceptable and unacceptable usage of Cognizant and Cognizant's clients' information and information technology resources. This policy is to serve as a critical reference point in decision-making when operating in a globally diverse work environment.

Corporate Security is committed to function as a true business enabler, by aligning our security requirements to our business objectives. Together we should focus not only on achieving our business goals, but achieving them through consistent behaviors that reinforce our client's trust in Cognizant's integrity and the appropriate use of technology.

Security is everyone's responsibility - your role is critical.

Best regards,

Francisco D'Souza
Chief Executive Officer

Henry Shiembob
Chief Security Officer

Contents

Acceptable Use at Cognizant

This Acceptable Use Policy (AUP) sets forth the policy of Cognizant Technology Solutions Corporation and its direct and indirect subsidiaries (collectively, "Cognizant") with respect to the acceptable and unacceptable usage of all Cognizant's and Cognizant's clients' information technology. Appropriate use of Cognizant and Cognizant client information technology resources is critical to comply with our legal and contractual obligations, ensure the delivery of our services, protect our confidential information, and safeguard the integrity of our data. Violations of this policy can result in serious reputational, legal and financial harm to the company, and potential disciplinary and/or legal action against individual violators up to and including termination.

To whom does this Policy apply?

All Cognizant information technology users, which include Cognizant Associates, contractors, consultants, partners, suppliers, service providers, interns and Cognizant client Associates (the "Users"), who work at Cognizant facilities, Cognizant client sites, and/or any other locations where the technology is accessed.

All information technology and associated information are owned by Cognizant and/or Cognizant's clients and must be used only by authorized users for legitimate business purposes. By accessing information technology assets, users are consenting to monitoring as permitted by applicable laws. Cognizant and/or Cognizant's clients reserve the right to perform the following activities in accordance with and to the extent permitted by applicable local laws and regulations.

- Monitor the use of information technology assets, including retrieving, reading, inspecting any information, to identify or investigate inappropriate access and use, and for other business purposes.
- Block any communication containing information that may cause negative business, financial, privacy, and/or public relations impact from leaving the organization.
- Search the personal belongings of anyone entering or leaving Cognizant or Cognizant's clients' premises for security purposes.
- Establish and undertake disciplinary actions for unauthorized exceptions (violations) to the policy, as detailed under the Enforcement section below.
- Confiscate information technology assets, if used in violation of Cognizant policies, contractual obligations and/or applicable laws.

What is covered in this Policy?

All information technology managed assets, owned, leased, contracted, administered, maintained, hosted or otherwise under the responsibility of Cognizant or which are used to deliver services to Cognizant. Additionally, this policy covers any information technology that is used to store, process, transmit or access Cognizant or Cognizant client information.

Information technology assets include, but are not limited to, servers, desktops, laptops, external storage devices such as USB drives, CD/ DVDs, portable hard disks, tapes and floppy disks, printers, fax machines, telephones (PSTN and VNet), access card readers and mobile devices (such as company-provided, Cognizant client-provided or personal PDAs), BlackBerries, cell phones, smart phones and wearable technology). Information technology services include, but are not limited to e-mail, internet, voicemail, networks, public cloud based services such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) or Software as a Service (SaaS) and any other applications.

Our Commitment as Cognizant Users

Users must understand and comply with this Acceptable Use Policy - including policy statements, standards and guidelines.

Users must fully cooperate with the Corporate Security team and employees of other departments (e.g. Human Resources and Compliance) on all investigations and all requests from Corporate Security. Please note that Corporate Security is the only team authorized for performing investigations involving Cognizant Associates. Failure to inform Corporate Security of an incident, or self-investigation of an incident will be viewed as a direct violation of this Policy.

In addition to complying with the standards set out in this policy, users are expected to behave consistent with the spirit of this policy, and local laws and regulations, including situations where a specific circumstance is not explicitly defined within this Policy.

Incidental Personal Use

Incidental personal use of information technology assets is permitted, unless explicitly prohibited by the Cognizant client or by the specific Cognizant organization. Such prohibitions must be communicated to users separately from the AUP. Incidental personal use of information technology assets is limited to users (i.e. Associates) and does not include family members and others who are not affiliated with Cognizant. In addition, such incidental personal use of information technology assets is only permitted provided it does not violate legal or regulatory requirements, Cognizant client contract requirements, Cognizant's Core Values and Standards of Business Conduct[1] ("Code of Conduct") and applicable security policies, standards, procedures and contractual requirements.

Reporting a Possible Violation or Incident

All suspected violations of this policy must be reported to the Corporate Security team, unless otherwise mandated by local laws (e.g. France, where the country laws require local reporting), regardless of whether the violation occurred at a Cognizant location, at a Cognizant client location or at some other location where Cognizant's or Cognizant client information technology was utilized or affected. The Corporate Security team is responsible for investigating violations of this policy. Suspected violations of this policy must be reported to the Corporate Security team as follows:

Phone: Option zero on VNET: 56666 | US Toll free no: 1-866-822-2024 | UK Toll free no: 0800-678-1616 | India Toll free No: 1800-2000-473)

Online: https://corporatesecurity.cognizant.com/Pages/reportIncidents.aspx

[1] The Cognizant Core Values and Standards of Business Conduct may be downloaded from https://corporatesecurity.cognizant.com/Policies/COBE.pdf

Email: csirt@cognizant.com

You may also report a violation anonymously (subject to certain country-specific laws and regulations, which in some cases prohibit anonymous reporting) through Cognizant's Compliance Helpline by filing a report, either by phone or via the Internet. Instructions for filing a report through our Compliance Helpline are contained in our Code of Conduct.

Policy Exceptions

While this policy requires strict adherence, there may be special circumstances where an exception may be appropriate. Exceptions to this policy will only be granted if the exception is approved through the formal exception management process. Exceptions may be requested via the policy exception section of the Corporate Security website (https://corporatesecurity.cognizant.com) or via email to corporatesecurity@cognizant.com. Exceptions will be assessed based on the business impact and the security risk that the proposed exception may pose.

Enforcement

Violations of this policy and any applicable Cognizant client policies, standards or procedures may result in disciplinary action up to termination and/or legal prosecution under the provision of local laws. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Cognizant. All Cognizant Associates are required to report, all known suspected or actual violations of this policy. Managers who direct or authorize conduct in violation of this policy, or who have knowledge of such conduct and do not immediately report it, may also be subject to disciplinary action as described above.

Acceptable Usage Standards

Information Technology Handling

- Users are responsible for all information technology assets and associated information assigned to them and must use them for legitimate business purposes only.
- Users must properly access, classify, label, store, handle, and securely destroy/dispose information technology assets and associated information under their responsibility when no longer needed, as per the Information Classification and Handling Standard[2] (and all other applicable company policies and standards).
- Access to information technology and associated information must be authorized and restricted only to those users that need access for legitimate business purposes.
- Users must ensure that before any confidential, sensitive and/or Personally Identifiable Information (PII) is shared within and/or outside Cognizant:
    - A formal approval process is followed
    - The information is used for the intended purposes and is shared in accordance with applicable corporate policies and standards, Cognizant's clients' policies and standards and local legal requirements as applicable.
- Users must follow the clean desk policy and must not leave confidential, sensitive and/or Personally Identifiable Information (PII) on printers, white boards, in conference rooms, work spaces, offices, and cabins/cubicles. All such information must be removed or securely locked in cabinets when users leave the work area. Also, users must securely handle confidential, sensitive and/or Personally Identifiable Information (PII) and information technology in public places like hotel rooms, cabs and airports.
- Users must lock computer screens when leaving their workstations (ctl-alt-del, lock screen).
- Users must safeguard access cards/tokens and access information such as IDs and passwords.
- Users must return all Information technology assets upon leaving Cognizant's employment or when the user experiences a change in job responsibilities where

[2] The Information Classification and Handling Standard may be downloaded from https://corporatesecurity.cognizant.com/Policies/ICHS.pdf

the information is no longer required (including all electronic and paper information belonging to Cognizant or Cognizant's clients). Managers must report assets which are not returned or are unaccounted for as a result of an assigned user's job change.

Users must **NOT**:

- Make any use or perform any activity that, in Cognizant's reasonable judgment, involves, facilitates, or attempts any of the following:
  - sending or posting discriminatory, harassing, defamatory, or threatening messages or images on the Internet, via Cognizant or the client's email service or on internal Cognizant or client hosted environments;
  - violating any law of, or committing conduct that is tortious or unlawful in any applicable jurisdiction;
  - gambling activities;
  - displaying, querying, performing, sending, receiving or storing any content that is obscene, pornographic, lewd, lascivious, or excessively violent, regardless of whether the material or its dissemination is unlawful;
  - advocating or encouraging violence against any government, organization, group, individual or property, or providing instruction, information, or assistance in causing or carrying out such violence, regardless of whether such activity is unlawful; or
  - propagating chain letters or pyramid schemes, whether or not the recipient wishes to receive such mailings.
- Sabotage or disrupt access to or the operation of information technology and/or any associated information.
- Create, distribute or execute any virus, worm, malicious code, spy-ware, backdoor hacking tools, password cracking tools, sniffers, network scanning tools, keystroke loggers and Trojans.
- Modify or circumvent any Cognizant or client-provided security controls, including but not limited to, authentication and Data Loss Prevention (DLP) controls, regardless of intent without an authorized written exception from Corporate Security.
- Access assets and associated information using someone else's identity, access cards, tokens, IDs or passwords.
- Share or reveal account passwords to others including co-workers, vendors, suppliers, clients, friends or family members.
- Allow the use of Cognizant information technology assets by others including, but not limited to, family and other household members when work is being done outside Cognizant or client locations.
- Copy or post copyrighted materials (for example, those items covered under the Digital Millennium Copyright Act), source code, project artifacts and other information outside Cognizant's and/or the client's network.
- Move client confidential information out of the client's network into the Cognizant network without the express written permission of the client.
- Attempt any unauthorized access to information technology resources.

- Connect to any non-Cognizant networks (i.e. connecting to a guest Wi-Fi, personal cell phone hotspot, etc.) while connected to the Cognizant network.
- Send any information to non-client accounts including personal accounts (like Gmail) and Cognizant account, when connected to client network.
- Use any program, script or command with the intent to interfere with or disable the proper operation of information technology.
- Execute any form of system or network monitoring outside the user's job function.

If you are unsure about what constitutes acceptable usage or activities, you should ask a member of Corporate Security or Compliance for further guidance and clarification.

Software Installation and Maintenance

- All software installation must be strictly for business use only and must be authorized via standard business unit software authorization procedures.
- Users are responsible for content that exists on their desktops and laptops.
- All software installations must comply with Cognizant software license compliance requirements, patents, copyrights and trademarks and protection of intellectual property rights.

Users must **NOT**:

- Uninstall, disable or interfere in any way with security software and tools including, but not limited to, anti-malware, password-protected screensavers, data loss agents or security logs.
- Use or possess password cracking programs, security vulnerability assessment, exploitation tools, or network sniffers to capture and view transmitted data, network discovery tools, system discovery or inventorying tools.
- Download or distribute pirated software, games, movies, songs, or pictures.
- Download, install or distribute unauthorized software (including trial software), freeware, shareware, open source software, games, audio, video or similar executable files from the Internet or other external sources.
- Make modifications to any software without permission of copyright holder.
- Access, download or use any third party software violating the software vendor's license requirements.
- Make use of code protected by license without complying with the terms of the software license (i.e. placing restricted code snippets in client code).
- Export software, technical information, encryption software or technology, in violation of export control laws.
- Use a personal software license for business purposes on Cognizant owned information technology assets.

Email and Communication

- Users must use appropriate secure transmission (password protection, encryption, digital signatures, etc.) methods for all confidential information transfers.
- Users should only send emails to business accounts unless there is an legitimate business reason to send them to personal accounts (i.e. HR communications to external candidates)
- Users must exercise caution when opening e-mails, e-mail attachments or links from unknown sources or of suspicious nature. Attachments in suspicious emails should not be opened and the suspicious emails should be forwarded to reportspam@cognizant.com.
- All communication in social media must follow Cognizant's Code of Conduct as well as Cognizant's Social Media Guidelines[3].
- Users should inform conference call participants if the call is going to be recorded.

Users must **NOT**:

- Send Cognizant or client confidential information to personal email accounts.
- Attempt to eavesdrop or join conference calls without being invited.
- Send emails from client email IDs to Cognizant or non-client email domains without client authorization.
- Use personal accounts for business communications.
- Upload confidential information to non-business domains.
- Attempt to intercept or access electronic messages that belong to other users without approval of Cognizant's Legal Department.
- Use client names, client logos, project names, project details or any other identifying information in external presentations, discussions, social media or professional networking sites without approval from Cognizant's Corporate Communications team.
- Disclose confidential and/or sensitive information related to Cognizant and clients to Internet groups, mailing lists, blogs and other Internet forums.

Physical Security

- Users must wear and display their photo identity / access card within workplaces as required by applicable Cognizant or client policies.
    - Users must never share their photo identity / access card or physical keys with other Associates.
    - Lost or stolen photo identity / access cards must be immediately reported to Corporate Security, local Physical Security POC and supervisor.
- Users must ensure that equipment such as laptops and other mobile devices and associated information are safeguarded and remain within their control at all times

[3] Cognizant's Social Media Guidelines may be downloaded from https://corporatesecurity.cognizant.com/Policies/SMG.pdf

whether in office locations or public places such as airports, restaurants, conference centers, etc.
- If any Cognizant or client supplied equipment is lost, damaged, misused or stolen, users must immediately notify their supervisor/business unit heads and report the same to the Corporate Security team.
- Users must ensure that confidential, sensitive and PII is physically secured wherever applicable.
- Users must utilize crosscut shredders, or Cognizant provided shredder bins, to dispose confidential, sensitive and PII information.
- All visitors, contractors, consultants, etc must follow local visitor management processes and must be accompanied by a Cognizant Associate at all times while on Cognizant property.

Users must **NOT**:

- Attempt to access unauthorized areas.
- Users must not leave equipment such as laptops and other mobile devices unattended in vehicles or other locations where they can be accessed, taken or stolen by third parties.
- Tamper with, circumvent or deface Cognizant physical security controls (like access control devices and CCTV)
- Take photographs or videos inside workplaces.
- Share access or identity cards or physical keys to Cognizant property.
- Tailgate (following a person to a restricted area) through access doors or encourage tailgating.

Incident Handling

- Users must disclose any suspected or actual unacceptable use of Cognizant or client assets to Corporate Security.
- Users must promptly report any security weakness or incident that violates any applicable security policies, standards or procedures.
- All client requests for information associated with an incident or an investigation must be forwarded to Corporate Security.
- Failure or delay in reporting an incident/violation to Corporate Security or self-investigating such an incident will be viewed as a direct violation of this Policy.

Users must **NOT**:

- Cooperate with or direct Associates to cooperate with client-initiated investigations without notifying Corporate Security and obtaining appropriate approvals from Cognizant's Legal Department.
- Modify or delete any information (i.e. emails, logs, files, etc.), evidences or audit trails related to a security incident or investigation.
- Notify parties that they may be the subject of a security incident or investigation without authorized permission from Corporate Security.

Personal Devices

Personal Devices include any Information technology that is not Cognizant and/or client provided. This includes, but is not limited to personal desktops, laptops, tablet devices, smartphones, wearable smart technology, thumb drives, etc. Personal devices fall into three categories:

- Personal Computing Devices: Devices with an enterprise operating system (Windows XP/7/8/10/RT, Linux, Chrome OS, OSX, etc.)
- Mobile Computing Device: Tablets and mobile phones running a mobile operating system (Windows Mobile, iOS, Android, etc.)
- Personal Storage Device: Devices capable of storage (smartphones, thumb drives, mobile computing devices capable of storage, flash memory, external hard drives, optical disk writer, etc.)

Mobile Computing Devices may be enrolled in Cognizant's Mobile Device Management (MDM) program. Enrolled devices may be used to access Cognizant networks or data via authorized MDM applications including email and applications delivered via the secure application store.

Users must **NOT**:

- Connect personal devices to the Cognizant Corporate Network or customer network (including but not limited to Remote Access VPN, wired LAN connections within Cognizant locations and Corporate (non-guest) WiFi connections within Cognizant locations).
- Bring Personal Computing Devices into Cognizant premises without prior approval. All Computing Devices brought into Cognizant facilities must have a visible asset tag issued by either Cognizant or a client company.
- Use personal devices to access, send, receive or store Cognizant business records or confidential information including client confidential information (this does not apply to personal device use permitted above).
- Use personal devices to circumvent security controls designed to protect Cognizant and/or client data and systems.

Note: Individual facilities or delivery centers may have additional prohibitions over and above these requirements. Associates are responsible to ensure that they are not in violation of any additional local restrictions on the possession or use of personal devices.

Public Cloud-Based Service Use

- Users may only use public cloud services that have been approved by Corporate Security
- Public cloud-based services that have been formally approved by Corporate Security must be configured to meet the minimum control standards outlined in this document:

https://corporatesecurity.cognizant.com/Policies/Corporate_Security_Policies/Standards/QSIS-MINSEC.pdf

- Corporate Security will be provided read-only access to all public cloud accounts for governance purposes unless it has been contractually agreed to otherwise such as may be the case in client-hosted environments.

Users must **NOT**:

- Use personal public cloud-based services to store Cognizant or client confidential information.
- Use public cloud-based services to circumvent Cognizant and/or client security controls.
- Store client data in public cloud-based services without explicit written permission from the client.

Zero Tolerance

Cognizant prohibits the use of information technology assets to engage in harassing or discriminatory behavior that violates Cognizant's Code of Conduct. Failure to abide by these policies may result in disciplinary action and/or termination of employment as permitted by the local law. Users may not use information technology assets to:

- Initiate or become involved in physical or verbal altercations, propagate ethnic slurs, deliver personal insults, obscenity, engaging in discriminatory, defamatory or harassing actions based on someone's race, gender, age, nationality, or other personal trait or characteristic, or other such conduct that is not consistent with proper professional behavior and that may be precluded by company policies and standards, clients' policies, standards and workplace rules, and local laws as applicable. The aforementioned inappropriate behavior is not only precluded in Cognizant and clients' sites, but also in any venue where Cognizant Associates, contractors, consultants, partners, suppliers, service providers, interns and/or client Associates congregate for a business related purpose such as hotels, conference centers, restaurants, etc.
- Access, download, transmit, store, copy or display offensive, sexually explicit, profane, racist, defamatory, intimidating or unlawful materials or content related to gambling, illegal weapons, terrorist and/or any other illegal activities.
- Use language that may be considered sexually explicit, profane, racist, offensive, or defamatory.

- Communicate messages that may be considered disrespectful, hostile, violent, intimidating, threatening, or harassing.
- Make fraudulent offers of products, items/services.
- Make statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Use Cognizant or client property or information, or the user's role within Cognizant or the client to compete with either Cognizant or a Cognizant client directly or indirectly.
- Use client-supplied property or assets, including software, for a different company or for a different client within Cognizant.
- Solicit or make offers of products or services offered by Cognizant or its client outside the user's job responsibility.
- Use information technology assets to support any activity, which represents an actual or perceived conflict of interest as defined in Cognizant's Code of Conduct.

Dissemination and Amendment

These Standards mentioned in the policy will be distributed to each Cognizant Associate upon commencement of his or her employment or other relationship with Cognizant and will also be available on the company's intranet. All Cognizant users shall certify no less than once during each 12-month period that he or she has received, read and understands the standards set forth in this policy and will comply with its terms. Cognizant reserves the right to amend, alter or terminate these standards at any time for any reason.[4]

[4] A current copy of this policy may be downloaded at https://corporatesecurity.cognizant.com/Policies/AUP.pdf

Glossary

Confidential Information:

Information belonging to Cognizant or Cognizant's clients including (but not limited to) client names, project names, pricing, patents, trade secrets, copyrighted information, source code, software design, billing rates, contract details, marketing information, financial and legally privileged information and salaries other than your own. Confidential information includes PII.

Personally Identifiable Information (PII):

Information that can be used on its own or with other information to identify, contact, or locate a person, or to identify an individual in context, and may include names, addresses, e-mail addresses, phone numbers, taxpayer or national ID numbers, healthcare information, or banking or credit card information. PII includes sensitive information.

Sensitive Information:

Sensitive Information is a subset of PII and it covers Information that reveals the age, race, ethnicity, sexual orientation and sexual life, political views, gender, physical or mental health or condition or disability or religion or similar belief, trade union affiliation of any individual or the commission or alleged commission of any offence by such individual or information about any proceedings for any offence committed or alleged to have been committed or disposal of such proceedings (including sentencing information).

Public Cloud Services:

Services made available to users on demand via the Internet from a cloud computing provider's servers as opposed to being provided from a company's own on-premises servers. Cloud services are designed to provide easy, scalable access to applications, resources and services, and are fully managed by a cloud services provider. Examples of public cloud-based services include, but are not limited to, Box, Dropbox, Zoho, Salesforce, Office 365, OneDrive, Google Drive, Amazon Web Services and Microsoft Azure. ***This list does not constitute approved software or vendors and is for illustrative purposes only***.

Document Revision History

S.No	Date	Version
1	November 01, 2004	V1.0
2	August 05, 2005	V1.1
3	November 03, 2006	V 2.0
4	October 04, 2008	V 2.1
5	January 09, 2009	V3.0
6	June 08, 2010	V4.0
7	December 11, 2011	V5.0
8	March 1, 2012	V5.1
9	April 5, 2013	V6.0
10	September 1, 2014	V7.0
11	October 9, 2015	V8.0
12	January 17, 2017	V9.0