Group **Cybersecurity**

ACCEPTABLE USE POLICY

December 2022

Company Confidential

Version:	5.0
Status:	Published
Usage:	For Capgemini Internal Use Only
Author:	Paul Thomas
Date:	01/12/2022

The Group Cybersecurity Framework

The Group Cybersecurity Framework defines the scope, governance, policies, standards, guidelines, and international standards necessary to implement the Group's strategy.

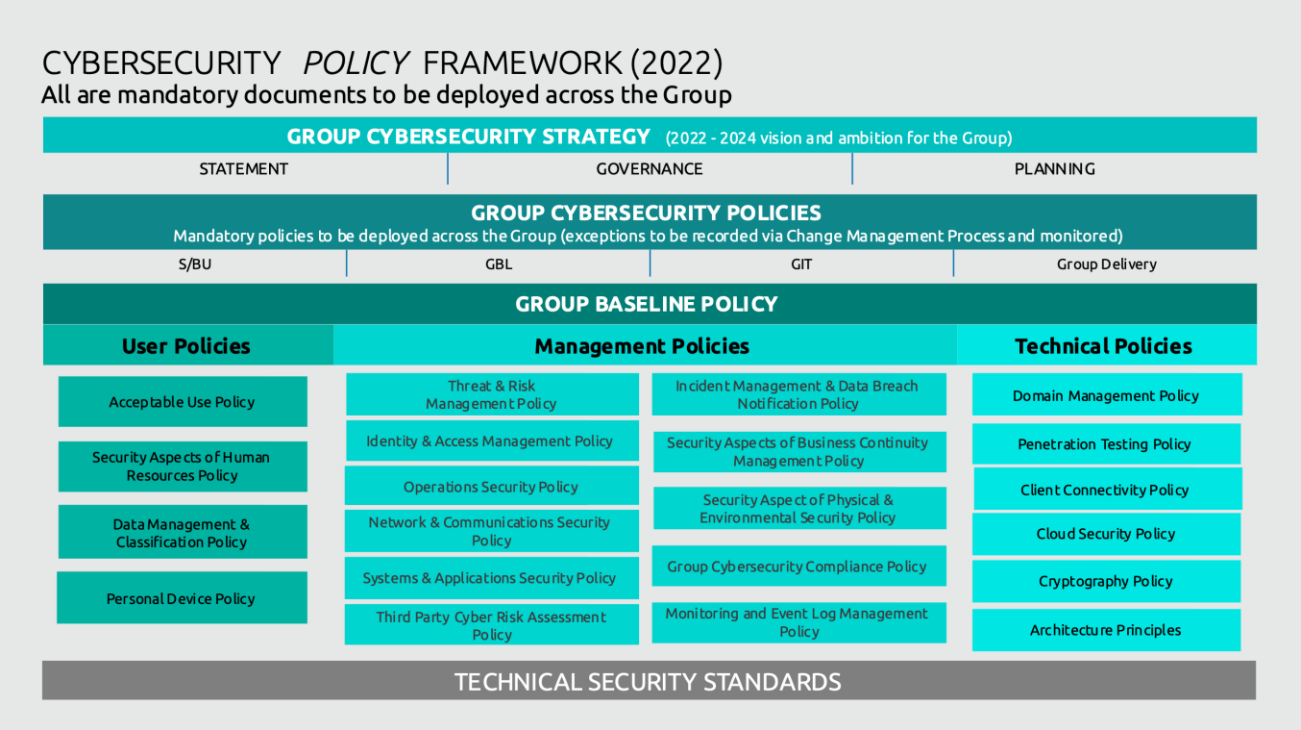
The Strategy presents the Group statement (vision and ambition), the governance (roles and operating model) and the planning. In particular, as a Digital Service Provider for many Essential Service Operators, our Group has to align with the NIS European Directive and equivalent in other regions.

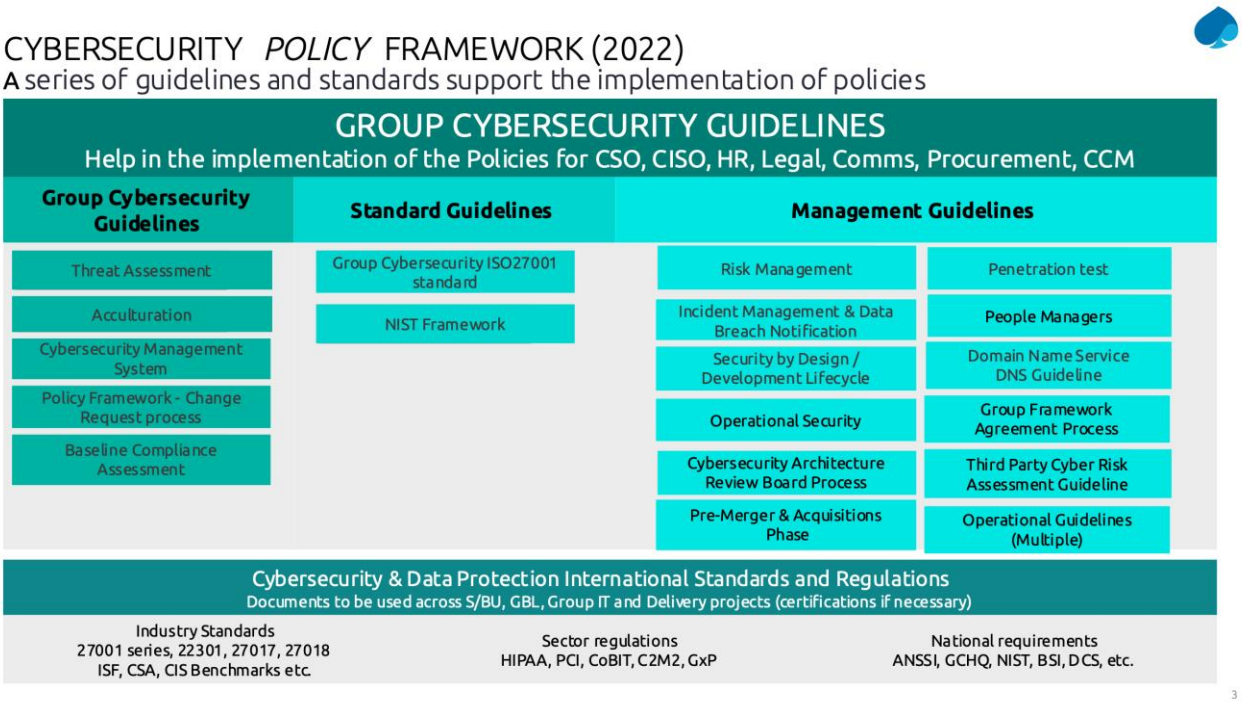
The Policies present "What" must be implemented to deploy the strategy, manage threats, mitigate the risks and control effectiveness of solutions and processes. They are built upon international standards and national security agencies requirements.

The Guidelines explain "How" to implement the policies depending on who is accountable or responsible for. Group Cybersecurity Office, SBU, BU and GBL have to implement the Framework consistently with strong collaboration with Group IT, Group Delivery and Global functions.

In addition to these documents, the Framework gives advices on the most important international and industry standards to be used by entities within the Group.

The diagram below presents the hierarchy of these documents which are published on Talent Group Cybersecurity Hub and updated at least once a year.





Contents

1 Purpose

The purpose of the Capgemini Group Cybersecurity Acceptable Use Policy (the "Policy") is to detail the acceptable and prohibited use of data, systems and information assets in compliance with Capgemini's established Code of Ethics (protecting confidential information, intellectual and/or industrial property, trade secrets, personal data, and usage of Group and third-party information assets and resources).

This document details the content and context for the information held within the mandatory AUP Awareness online training course to be completed by all employees.

Please note that this Policy shall be further complemented with the specific privacy policies and/or notices that address the collection and subsequent processing of personal data that may derive from the acceptable uses recognized herein.

2 Definitions

Acceptable Use	is further detailed in this Acceptable Use Policy but, in general, shall refer to the reasonable and proportionate use, with the utmost care and diligence, as carried out in compliance with the AUP, and which does not interfere with professional duties or tasks and does not create undue risks of damage
Assets	refers to devices and/or resources including, but not limited to, laptops, smartphones, tablets, desktop computers etc., as well as other information systems and networks, tools, data sources and other related technology components
3rd Party Assets	refers to devices and/or resources (as for assets) but provided by a 3rd party for Capgemini employee use in support of delivery of the intended purpose
Data	Data is all information (including personal data as Data Controller and/or Data Processor), created, stored, transmitted within Capgemini and outside of the company to partners, providers who support our business operations and where we act as Data processor for our clients or create, store and transmit information as part of our business operations with our clients
Data Assets	Are all systems and applications that process store or transmit data, such as Applications – for the processing of Data E-mail – for transmission of Data Databases – for storage of Data External Hard drives / USB data sticks – for storage and transportation
IT Assets	Are technology assets that support data assets, such as Hardware - CPU (central processing unit), Drive, Modem, Motherboard, Network card, RAM, Storage device. Software – Windows, Android, Linux, Kernel Middleware - Platforms for executing business transactions, Data access, Database access services, Application Frameworks, Device Middleware
Capgemini Information	Is all information, created, stored, transmitted within Capgemini and outside of the company to partners, providers who support our business operations and where we act as Data processor for our clients or create, store and transmit information as part of our business operations with our clients.
Capgemini or **Group**	refers to any and all legal entities / affiliate(s) of Capgemini SE.
Monitoring tools	Monitoring tools are used to continuously keep track of the status of the system in use, in order to have the earliest warning of failures, defects or problems and

	to improve them. There are monitoring tools for servers, networks, databases, security, performance, website and internet usage, and applications (as well as other scenario's).
Multi-factor authentication	Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g. password/personal identification number (PIN)); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).
Personal Device	Is any device owned by an Employee used to connect via approved means to the Capgemini infrastructure
Fully Managed Device	All devices: - Supplied by Capgemini i.e. Company owned device supplied and fully managed by Group (IT Supplied asset / computers etc), where Capgemini Group IT fully manage the personal device i.e. everything is under the management control of Group IT
Partially managed Personal Devices	Personal devices where the device connect via the Group IT Solution and Group IT manage a part of the device (the container section). The Capgemini container solution is control under the control of Group IT and the container segment can be wiped remotely without effecting the personal area of the device.
Unmanaged Personal Devices	No control or capability for Capgemini to on the device even partially with restricted and controlled access to a limited set of corporate and Client applications (where a client is involved – this must be in compliance with Capgemini's contractual obligations.
Pentest	A Pentest is a security testing in which pentesters mimic real-world attacks (ethical hacking) to identify methods for circumventing the security features of an application, system, or network. It often involves launching real attacks on real systems and data that use tools and techniques commonly used by attackers. A pentest can be defined as an "ethical hacking" initiative to test for vulnerabilities and weaknesses.
Red team activity	A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve enterprise cybersecurity by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment. Also known as Cyber Red Team.
Social Engineering	An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems, networks or obtain data.
Users	An Individual authorized to access an Information asset, systems and infrastructure to undertake the activity they are employed for.
Security Incident	Security Incident Is defined as "any event having an actual adverse effect on the security of network, information systems" and / or Data.
Information Cybersecurity incident	Single or a series of unwanted or unexpected Cybersecurity events that have a significant probability of compromising business operations and threatening information security
Information Cybersecurity event	Identified occurrence of a system, service or network state indicating a possible breach of Cybersecurity policy or failure of Group Cybersecurity controls, or a previously unknown situation that may be security relevant.

In addition to the terms defined in the above table, you can also refer to the CYBERSECURITY GLOSSORY OF TERMS AND DEFINITIONS

3 Scope

This Policy applies to all who are granted access to Capgemini assets, on the basis of their employment contract with Capgemini. Exceptionally, other parties may act on behalf of Capgemini and receive access to select corporate assets. These parties shall be also bound by the rules laid out in the AUP without implying nor creating any employment relationship between Capgemini and these other parties (e.g. subcontractors, etc.). (Hereafter collectively referred to as the "Users" or individually as "User")

All contents in this Policy are contractual and form part of your terms and conditions of employment with the Company. Please read the Policy carefully as failure to comply with the standards set out here could result in disciplinary action.

Capgemini provides electronic information and communications systems to facilitate its business needs. These systems include, but are not limited to, infrastructures, networks, computer equipment, software, applications and online services, operating systems, storage media, computer networks, electronic mail, voicemail, telephone, digital tablet and equipment, file servers, databases, etc. that are owned or leased by the Company.

In addition, the Policy applies to all Assets owned or leased by Capgemini that are used by Users and to any devices that connect to a Capgemini network from Capgemini locations or remotely along with access to information / data (either of Capgemini and/or its clients). It also covers the requirement relating to client provided devices (please refer to contract for client specific AUP that may apply), access to delivery services and for all Users using their own devices (when approved to do so) in line with the Personal Device Policy.

4 Synopsis

This AUP document is an integral part of the Group Cybersecurity Framework covering the most important behaviors about what users are, and are not, allowed to do in relation to our services, with Data, information and Data systems / IT systems of our organization.

This Policy document outlines the rules to be applied relating to key areas where Capgemini requires its employees to act accordingly to protect our company and our company's and clients' reputation.

It details what employees are and are not allowed to do, what is considered as both acceptable and unacceptable behaviors with the objective that all our employees use and handle information and systems securely.

5 Responsibilities

The Assets are to be used, always with the utmost care and diligence, and for business purposes of Capgemini during normal business operations. Effective security in using the Assets requires the participation and support of **all** Users granted access to the Systems and Information.

We are all responsible for safeguarding business information and other assets under our control and aware of the Group Cybersecurity Policy Framework, to behave according to it and to conduct our activities in a professional and responsible manner.

Every manager is accountable for security in their business unit and adherence to Company security policy and standards.

Enforcement of the Acceptable Use Policy is via the Human resources Disciplinary process where identified. Other actors (e.g., SBUs, Cybersecurity managers, Delivery managers and Users) can oversee specific controls when IT assets are provided to you or by clients or third parties (e.g. Cloud services, Social media services, etc.). It is the responsibility of all Users to follow this Policy in their area of operation.

For security and network maintenance purposes, authorized individuals within Capgemini may monitor equipment, systems and network traffic at any time as described in section 12 of the present Policy.

6 Appropriate Use of Group Assets and Resources

Users are personally accountable for the protection of the Group and third-party Assets and resources under our control as defined in the Group Ethics Policy.

WHAT DOES THIS MEAN?
Responsible and professional use. Users use assets and resources that belong to the Group to help us achieve our business goals. User's obligations include but are not limited to:

- Users take care of third-party assets and resources as if they are our own.
- Users must not access, use or attempt to use Group or third-party electronic resources to access, store, send, post or publish material that is inappropriate. This includes material that is pornographic, sexually exploitative, obscene, racist, sexist or in any other way discriminatory, threatening or harassing, personally offensive, defamatory, related to terrorism, political or illegal.
- Users are expected to take the necessary steps to protect any assets and resources of the Group and/or third parties', including clients' which are under our control against loss, theft and unauthorized disclosure.

WHAT IS EXPECTED OF USERS?

- Users take care to protect Group and third-party assets and resources.
- Users must use the Group's physical and electronic resources only for business purposes, except for exceptional circumstances in which personal use is permitted for the minimum time required and to the extent that such use does not interfere with my work responsibilities and/or tasks and does not put the Group's assets at risk of any damage.
- Users acknowledge that use of the Group network only to transmit or store material is under the control of the Group.

Please note that the list above is indicative and is not exhaustive.

In addition, Users are expected to read, understand, and abide by their local Country Cybersecurity or any other user relevant user policy covering country specific legislation and regulation, particularly the Personal Device Policy, and any other client cybersecurity and acceptable use policies where applicable.

6.1 Accessing Information Systems and Network

Users must:

- Secure all Capgemini supplied assets and Personal devices when used to connect to Capgemini infrastructure, including, but not limited to laptops, smart phones and desktops with a strong password according to the Cybersecurity Policy – Identity and Access Management (Client-specific requirements must also be met in line with contractual obligations and, where applicable, client-specific AUPs);
- Keep passwords and authentication devices and/or applications (e.g. two-factor / multi-factor) strictly confidential, securing the authentication device at all times;

- Where not controlled by Single Sign-On service, set different passwords for different Application access needs; use stronger, more complex, passwords for more sensitive systems and confidential documents.

6.2 Email and the Internet usage

Company employees are expected to use the Internet and email systems responsibly and productively, in pursuance of their business goals and objectives. Email and Internet access is provided for job-related activities, while limited personal use is allowed, it should only be permitted as long as such use is reasonable, proportionate, fully compliant with this Policy, and does not interfere the employees' professional duties or tasks.

Users must ensure that:

- Emails sent via the company email system do not contain content that is deemed to be offensive. This includes, though is not restricted to, the use of vulgar or harassing language/images or sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities.
- Unacceptable use of the internet by employees includes, but is not limited to sending or posting information that is:
    - defamatory to the company, its products/services, colleagues and/or customers
    - discriminatory, harassing, or threatening messages or images on the Internet
    - passing off personal views as representing those of the organization
    - Sharing confidential material, trade secrets, or proprietary information outside of the organization
    - Engaging in any illegal activities using the Internet.
- Only approved software (Group licensed software) is installed and used. Any other required software must be formally approved. The installation and use of any unauthorized software such as, among others, instant messaging technology, Internet browsers and browser plugins is strictly prohibited, as well as the downloading, copying or pirating software and electronic files that are copyrighted or otherwise protected against unauthorized reproduction, use or dissemination, is also forbidden. The use of unauthorized software may expose our organization and/or our clients to legal and security risks, insofar as such products (even though these may be subject to valid but personal licenses) may not provide sufficient security measures or contractual safeguards including sufficient liability coverage.

  Capgemini assets and resources are not to be used, under any circumstance, to perpetrate any form of fraud, and/or software, film, or music piracy, hacking into unauthorized websites, introducing malicious software onto the company network, or engaging in crypto-mining activities and/or jeopardizing the security of the organization's electronic communications systems, and/or the confidentiality, availability or integrity of the information stored or exchanged through such systems.

- Certain sites and downloads may be monitored and/or blocked by Capgemini if they are deemed to be harmful, illegal, or otherwise unacceptable, incompatible, or unsafe for business use. Where an employee uses Capgemini equipment or resources for personal use, the employee should mark as Personal, e.g.
    - Email – Mark the email 'Personal' in the Subject
    - For Storage – Mark the file 'Personal'

Email Users must:

- Use extreme caution when opening e-mail attachments received from unknown senders or even known senders that might look suspicious, which may contain malware.
- Be aware of phishing attacks in malicious e-mails which try to get a User to divulge a password or any other kind of confidential information.
- Forward suspicious email from an unknown sender and/or any suspicious spam email containing a link or attachment that seems unusual using the email ribbon Report Spam-Group IT icon or to CORP, spam box (spambox@capgemini.com); don't click the link or open the attachment.
- Never send any information or document related to clients or Capgemini to a private mailbox, or transfer onto your personal devices or cloud storage accounts,
- Not use Capgemini email system in a way that may be interpreted as insulting, disruptive, or offensive by any other third party, or which does not comply with the Code of Business Ethics;
    - Never create or forward mass emails for professional or personal reasons;
    - Only use e-mail services provided by customers or partners exclusively for their business purposes;
    - Delete any e-mail from an unknown sender containing a link or attachment that seems unusual;
    - Avoid Sending Spam via e-mail, text messages, pages, instant messages, voice mail, or other forms of electronic communication;
    - **Do not** use any private, personal or company information in your out of office messages.
    - **Do not** disclose private, personal email for Capgemini professional use
    - **Do not** click on a link within an email or enter your credentials into a website unless you are absolutely sure that it is safe, and when in doubt ask before doing so.

Internet Users must:

- Be cautious when using internet: Blocking pop-ups, downloading files only from trusted and reputable sites, ensure antivirus is active at all times.
- Avoid publishing personal data or any other information on websites.
- Keep Separate the links between your personal details and your professional profile.

- Always check the URL, use HTTPS and be careful with keyboard mistakes in the URL you type (an attacker can use fake similar URL to log you on evil sites).

- **Not** enter your credentials into a website unless you are absolutely sure that it is safe, and when in doubt ask before doing so.
- **Not** surf sites hosting offensive or inappropriate content.
- **Not** use public Internet transfer tools (e.g. MEGA, MediaFire, 4Shared and other similar platforms, only use Capgemini approved transfers tools e.g. File Transfer Service available on Talent)
- **Not** publish Client or Capgemini related data or information on Internet.

If an employee is unsure about what constitutes acceptable Internet or email usage, then he/she should ask his/her supervisor for further guidance and clarification.

6.3 Password Management

A password (including unlock codes or patterns, two-factor / multi-factor authenticators, tokens etc.) is your secret and must be kept as such, it is always your accountability to protect it at all times:

Users Must:

- Never share it with anybody or publish anywhere in any circumstance.
- Capgemini (Group IT, Group cybersecurity or your business units) will never need your password so do not disclose it.
- Never use the same password for different purposes. Every website that you privately use for ordering goods should have its own password to prevent abuse of your credentials if they are compromised. Private passwords / credentials must always be different from passwords used for Capgemini assets or applications for the same reason. Change your password regularly and immediately if you suspect somebody has seen you typing it or if you think it may be compromised in any other way.
- Strengthen your password by:
    - Making it longer, minimum 8 characters mixing letters numbers and characters (There are very powerful tools aiming at retrieving passwords by combining letters, symbols etc. Therefore, the longer and more complex the password the better).
    - Never use a password that is easy to guess (February2018, Capgemini123, 123@Capgemini, @dmin007, etc.) and avoid using dictionary words.
    - Take a phrase you can remember easily like: "I'm singing in the rain" or "it is a wonderful feeling" and convert it to something like: 1m$itR&i1aWF!

7 Using Social Media

Social media both inside and outside the Group have transformed the way we interact. Online collaboration enables people to share knowledge and ideas regardless of rank, title, or experience. It's a way for us to take part in conversations around the work we do at Capgemini and show our expertise in these areas.

While this brings huge benefits, it also comes with certain risks and responsibilities. The Group Social Media Code of Conduct sets out the full parameters for activity in this area, empowering engagement in social media but establishing the accountabilities that come with it.

The points below summarize the key requirements, but to be fully compliant, please complete the Code of Conduct training.

1. Do not share client information.

- Never share information around clients that is not in the public domain (e.g. already in a press release) including the names of clients or client employees, commercial information relating to a client's activities, or anything else that could be used to identify a client without express written permission.

2. Protect your colleagues.

- Do not share detailed information about team members' individual roles or contributions to specific projects; this may identify you and them to hackers as potential targets to attack Capgemini.
- Do not share colleagues' personal data, including their picture, without their permission.

3. Be secure.

- Use a secure password, update it regularly, and never share your login information with anyone.
- Do not use your corporate email address to create personal social media accounts.
- Never publish images of your company computer screen, security pass, or other identifiable security features.
- Don't click any links or download software on social media pages posted by individuals or organizations that you do not know and be cautious about clicking shortened URLs as these might also pose security risks.

4. Observe copyright law.

- Pictures, videos, copy, and other content owned by others must not be used for our own commercial benefit.
- Do not post links to other websites, posts, or pages without first checking that such sharing is authorized and that the content is lawful.

5. Be respectful.

- Never publish material that is obscene, racist, sexist, pornographic, sexually exploitative, or in any other way discriminatory, threatening or harassing, personally offensive, defamatory, or illegal.

6. Be transparent.

- Do disclose your association with Capgemini when discussing Capgemini matters.

- Always be honest about your role and position within the company; do not overstate your seniority and therefore authority.
- Don’t register personal accounts using the Capgemini name or brand name.
- Only authorized company spokespeople may represent Capgemini’s official positions online; be clear that you are expressing your own views and not those of the business.

7. Don’t criticize.

- Do not say anything disparaging about our business partners, competitors or colleagues.

8. Be constructive.

- Use social media to build relationships and share insights.
- Always respect the views of others, especially on topics of race, religion, politics, and gender.

9. Think before you post.

- However informal, content published online is shareable and searchable forever; even private posts can be copied and shared, potentially ending up in international media.
- Always assume that any personal social media activity can be linked by someone to your professional profile and therefore your employer.
- If in doubt, ask your manager or local HR representative before you post.

For more information about the Social Media Code of Conduct, please visit the Social Media Hub.

8 Social Engineering

Social engineering, in the context of information security, refers to manipulation of people / employees into performing certain actions or divulging confidential information.

Countermeasures to Social Engineering

- Do not be rushed into making a hasty decision, never allow an apparent urgency to influence your careful review and due diligence.
- Be suspicious of any unsolicited messages. If the message looks like it is from a legitimate company you use or are in contact with regularly, do your own research anyway. It may be the case that they were affected by a phishing attack, and you are receiving malicious messages that appear legitimate. Use a search engine to go to the real company's site, or a phone directory to find their phone number. When in doubt, always double check or report the message.
- Be wary of any unsolicited email and emails from unknown and unexpected sources.
- Be wary of any downloads or offers that just sound too good to be true.
- Delete any request for financial information or credentials (usernames, passwords) if you get asked to reply to a message with personal information.
- Delete requests for help or offers of help. Legitimate companies and organizations do not contact you to provide help.
- Do not be curious: overly curiosity can only lead to careless clicking.
- Similarly, never use or dial phone numbers included in the email; it is easy for a scammer to pretend and impersonate the intended recipient to make you believe you're talking to the right person.

9 Data Classification and Handling

Capgemini has a defined Group data classification policy to ensure a consistent approach to data protection across the Group and efficient allocation of security resources according to data asset value, covering:

- Physical: printed material or storage media.
- Electronic: data stored, accessed, or transferred via communication networks.
- Human: information verbally exchanged, either face to face or over the phone.
- Storage, in transit and destruction.

9.1 Responsibilities

All employees of Capgemini (Permanent, temporary and subcontractors) within Capgemini entities (accountable for creation, collection, processing and disposal) are responsible for performing Data / asset classification, with the help of the Business Unit Cybersecurity Officer, Data Protection Officer or Global Line of Business CISO if necessary, complying with the related data protection requirements.

- All users must respect the data protection requirements and apply the appropriate security controls as defined by the classification level. Particularly, users must apply the Capgemini Acceptable Use Policy.
- All users shall report inappropriate situations according to the Cybersecurity Incident Management process as quickly as possible.

Data must be classified under one of the four following categories. Applying the following rules is enough to classify information in most of the cases:

PUBLIC	Company Confidential	Company Restricted	Company Sensitive

SEC0: Public Information – By definition is information that is publicly available e.g. marketing collateral published via approved channels.

SEC1: Company Confidential Information - is all regular business owned and created by Capgemini employees which is not intended to be publicly available and only intended to be used by Capgemini internally.

SEC2: Company Restricted Information – This covers two scenarios

- Capgemini Restricted - Internal Capgemini Information that is intended for a restricted set of employees
- Customer Restricted - Information that is intended for a restricted set of employees with the right / need to know principle relating to a specific Account engagement where information owned by the client but managed by Capgemini or information related to customers and their environments (both Technology and Business related) is being handled. This Classification should be used for Capgemini documentation and systems where information is being shared with the client.

SEC3: Company Sensitive Information - is information, which is considered highly confidential, has regulatory controls that must be complied with and could damage the interests of the Capgemini Group or of the party to whom the information belongs if inappropriately disclosed. It again applies to a restricted set of employees on a need to know basis.

All documents should be marked with the appropriate classification (the Tags above can be used too). In addition, the rules / caveats can be detailed within the document to detail the intended audience, specifically for the Restricted and Sensitive classifications, detailing control instructions e.g. do not forward to unauthorized individuals, do not store in a shared business area, do not print etc.

For guidance on how to handle information in varying scenarios, please refer to the Group Cybersecurity - Cybersecurity Knowledge Center, and to the Group Cybersecurity - Data Management and Classification Policy.

10 Securing Your Workspace Environment

10.1 In the Office

Users must:

- Every employee must ensure that a security pass / badge is worn and visibly when on Company sites.
- Ensure all visitors / third party personnel are wearing a distinctive badge to be worn at all times, which will indicate clearly that they are a visitor. Ensure Visitors are escorted by their Capgemini Sponsor at all times. Be wary of any suspicious third parties that may be tailgating / piggybacking, and do not hesitate to challenge unfamiliar faces.
- Secure your Laptop: Always enable full disk encryption by shutting down your laptop completely at the end of the day and physically secure it, i.e. lock it away, use a lockable desktop base station or cable lock e.g. Kensington lock.
- Keep your desk neat and tidy to make data and equipment safe and secure in line with the Capgemini Clear Desk, Clear Screen Guideline, ensuring all confidential and Sensitive data is stored and secured in line with its Data Classification.
- Always lock your workstation or Laptop when leaving your desk (ctrl+alt+delete) to prevent unauthorized access.
- Keep physical documents and movable storage devices in a secured cabinet, in line with applicable data classification rules.
- Remove all confidential information from rooms, whiteboards etc. after meetings and dispose of all information, paper notes, flipchart papers and covers post meeting in a secure manner.
- Ensure secured collection of documents from printers in a timely manner.

10.2 Out of the Office (Mobility and Teleworking)

Ensure you protect your equipment and Company assets at all times.

Users must:

- Ensure Assets (laptops, smart phones, other media (holding company data), authentication devices are secure at all times and carefully supervised during travel or off-site work. Do not leave them in your vehicle or unattended in public locations such as airports, hotel lounges, cafés etc;
- Connect to the Company network from remote locations only through pre-defined authentication and authorization mechanisms established and approved by Capgemini;
- Never send any sensitive, Restricted and confidential information to your personal email, personal storage services (including cloud services such as Dropbox, Box, Google Drive, OneDrive, iCloud etc.) or transfer / download it onto your personal devices;

- Always dispose of equipment and media using the Capgemini disposal procedures;
- Strictly respect the Group Cybersecurity - Personal Device Policy.

10.3 Disposal

Users Must:

- All media must be destroyed in line with its Data Classification – Paper, Laptops desktops, removable media, disks, hard drives, external hard drives etc.
- Dispose of any confidential and sensitive information in a secure manner. Use confidential waste bins where they are supplied in Capgemini offices. Use paper shredder for documents that need to be destroyed due to the sensitivity of the information they contain.
- Equipment and media should be handed to your Group Real Estate representative or returned to Group IT for secure disposal / destruction of the information / Data being held on the media.

11 Devices

11.1 Capgemini Devices

User Must:

- Only use Equipment and Assets, any online services and software that have been formally approved by Capgemini Group IT. Exporting or importing software, technical information, encryption software, or technology in violation of international or regional export control laws and potentially Intellectual and/or Industrial property or licensing restrictions is Prohibited. Moreover, the use of unauthorized software (including online services) may expose our organization and/or our clients to legal and security risks. Unauthorized products, even though they are used with a personal license, may not provide adequate security measures or contractual safeguards including sufficient liability coverage that meets Capgemini standards and requirements.
- Implement and maintain the functionality of any security controls implemented by Group IT (laptop encryption, back up, authentication, anti-malware, screen savers, etc.); do not override, amend, circumvent, deactivate, and/or otherwise tamper with alter any of these security controls.
- Never use a Capgemini device to connect directly to Client data. Only ever use an approved connection method.

USB data and storage devices ports must be disabled (not other USB devices) and only enabled where there is a valid business requirements / contractual obligation for a users to store and save data and approved via the formal exception to policy process is available on ITaaS portal.

11.2 Personal Device Policy

This section is specific to Employees using their personally owned devices, where Capgemini has deployed a Capgemini Containerized solution (Partially managed device or the device is used to connect to the Capgemini Infrastructure (Unmanaged device).

The Personal Device Policy defines all the rules and requirements for using a Partially managed or unmanaged Personal device when connecting to Capgemini infrastructure and/or applications via Capgemini approved means, but specific requirements for users include the following requirements

Users Must:

- abide by the rules defined in the Group Cybersecurity Personal Device Policy which defines the rules to access Capgemini systems and Information remotely, using their own Personal Devices.
- abide by all the rules, regulations, policies and contractual commitments governing the use of Capgemini Information
- accept that for the protection of the Group's interests, for statistics and for quality of service only, Personal Device usage may be subject to monitoring by Capgemini at the point the personal device connects to Capgemini Infrastructure.
- access Capgemini Information from a Personal Device only with the authorization of your BU manager. This authorization is revocable always by Capgemini or your BU manager without providing reason and without prior notice.

- do not download and store Capgemini classified Information on your Personal Device . Always ensure you are using the approved Personal device Capgemini solution provided by Group IT.
- ensure that no third party has access to Capgemini Information through your Personal Device, including when your Personal Device is sent out for repair.
- Not connect to Capgemini network through unmanaged devices (devices not provided or approved by Capgemini or Personal Devices not secured with Capgemini approved secure container solution or approved connection method).

12 Additional responsibilities when using Company or client assets

The following practices are strictly forbidden when working for Capgemini or any Client's engagement without appropriate authorization:

- Circumventing user authentication on any device; or sniffing network traffic;
- Maliciously causing a disruption of service to either Capgemini or other network resources, including, but not limited to, ICMP floods, packet spoofing, denial of service, heap or buffer overflows, and forged routing;
- Intentionally introducing malicious code, including, but not limited to, viruses, worms, Trojan horses, e-mail bombs, spyware, adware, ransomware and key loggers; or Introducing honeypots, honeynets, or similar technology on the Capgemini network; Port scanning or security scanning on a production network unless approved in advance by Capgemini Security teams;
- Performing unauthorized Penetration tests and Red team activities on Capgemini applications and systems;
- Running virtual instances or containers on endpoints or outside data center or not supported and secured by required Group Cybersecurity standards.
- Forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the recipient about the sender;
- Use of a Capgemini e-mail or IP address to engage in conduct that violates Capgemini policies or guidelines;
- Engaging in crypto-mining activities.
- Posting
    - non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam);
    - to a public newsgroup, bulletin board, or listserv using a Capgemini e-mail or IP address without authority that represents Capgemini to the public;

- Violating copyright law, including, but not limited to, illegally duplicating or transmitting copyrighted pictures, music, video, and software;

- Using third party software on the basis of an individual (not corporate – CG) license in the performance of any professional duties either for Capgemini or any of its clients.

- Subscribing -
    - to e-mail lists which are not in the Company's interest;
    - to free webservices (Dropbox, Box, GitHub, GDrive, OneDrive, Yahoo, iCloud, Proton Mail etc.) using your company email address.
    - to personal networking sites using your company email address;
    - Note - Users Must "identify yourself" – when making a statement on behalf of Capgemini, You should identify yourself as being a member of the company.
- Posting content on any internet message board or other similar web-based service or any social networking sites that would bring the company or client into disrepute, or which a reasonable person would consider offensive or abusive;

- Using company or client provided systems or confidential information for personal financial gain.

- Hosting a personal web site on company equipment.

- Participating in online gaming activities or activating any web channel(s), or streaming services, that broadcasts frequent updates on computers, such as news broadcasts, match scores, etc. which may be regarded as grounds to consider that the employee is not performing his / her professional tasks and duties with the reasonably expected care and diligence.

13 Capgemini Monitoring

Capgemini has a duty to ensure, to the best of its capabilities, that our organization's business (including our infrastructure, Assets and information being managed and conveyed through said Assets, including those of our employees, clients, suppliers and other business partners are secure and safeguarded against any internal and/or external threats.

To prevent any occurrence of numerous threats and vulnerabilities and to aid the management of security incidents and breaches a level of monitoring is undertaken to identify cyber-attacks and prevent the introduction of malicious content or software that could be used by malicious individuals, which pose a risk to Capgemini's business and reputation.

For details of the measures applied (Specific Solutions) to protect the company and the reasons why they are applied, please refer to Appendix A.

Moreover, it is essential for Capgemini to monitor its Assets and where an Employee uses a Personal Devices monitor it solely at the point at which it connects to the company infrastructure to ensure that it does not introduce any malicious content to the company.

This is required to comply with Capgemini's legal obligations with regards to legislation and regulation, such as GDPR, European NIS Directive as well as to support evidence and proof where an incident does occur, in the case of controls by official authorities and/or legal proceedings that Capgemini may be part of in the case of the occurrence of an Incident.

The use of these tools and/or technologies may entail the monitoring and subsequent logging of the use of Capgemini Assets. It would therefore encompass the collection of information (including personal data) related to such use (for example, but not limited to, Asset-related information, device identification information, inbound/outbound connection information and other logging relating to the activity undertaken by the individual on the Capgemini environment).

The measures implemented to protect the company and the processing of information entailed by such measures are undertaken strictly when necessary for Capgemini to ensure the security of its networks, systems and applications and protect it against both accidental events and other unlawful or malicious actions that are continually evolving in their volume and complexity.

In furtherance of these objectives, Capgemini also needs to ensure that all employees / Users are aware of, and duly comply, with the requirements and obligations set out in this Policy, their applicable employment conditions and responsibilities, as well as any other applicable policies and procedures in force within our group.

The collection and subsequent processing of personal data resulting from this monitoring may be performed on different legal bases depending on the purpose pursued. Most commonly, processing activities described in this section will be performed on the basis of Capgemini's legitimate interest to run its business efficiently and securely and protect it against significant threats by preventing lapses confidentiality, availability and/or integrity of systems and information breaches of our Assets Information we manage and Data. For these purposes Capgemini assesses the necessity of such tools (or any others that may be implemented in the future while considering the relevant state of the art and the evolution of the risks to be addressed) and implements appropriate safeguards to guarantee a proper balance between our legitimate interest and the fundamental rights and freedoms of our employees / Users. In other cases, such processing activities may be performed where it is necessary for compliance with a legal obligation to which Capgemini is subject.

Since, in line with provisions within this [Policy], the use of Capgemini [Assets] for personal purposes is permitted in limited circumstances, the use of the abovementioned tools and technologies, some of which entail monitoring capabilities, may lead to certain minimal information (strictly related to the protection of Capgemini's infrastructure) being collected as a result of such personal use that [Users] make of the [Assets]. Due to the nature and objectives of some of the tools and controls that are implemented to ensure the comprehensive protection of our business, systems and networks against a plethora of threats and attacks, access to this information cannot be ruled out completely, even though Capgemini does not actively seek for this information.

In this sense, and in the context of such personal use, [Users] must be aware that the tools and technologies in place are never meant to monitor employee activity but focus on the protection of our networks and information systems against accidental events or unlawful or malicious actions that can lead to a compromise of the availability, authenticity, integrity and confidentiality of stored or transmitted information. As a result, such tools may not be able to technically discriminate between information originating from [Users]' professional or personal use (to the extent permitted) of our [Assets]. Notwithstanding this, Capgemini undertakes to implement any appropriate measures and safeguards to ensure that such access, even where merely incidental, has as minimal an impact as possible on the rights and freedoms of our [Users]. In particular, Capgemini commit to limit the access to such tools and technologies to staff members who have a strict need-to-know basis. Furthermore, any other access to personal data in these contexts must be subject to controls and approvals such as the ones of Group IT, HR, Data Protection Officer, Legal where relevant.

The protection of the dignity and privacy of our employees / Users] is paramount to our organization. Therefore, prior to considering and implementing any monitoring tool or technology in the terms described in this section, we make sure that such activity is always conducted in a proportionate manner, and that we implement adequate controls to minimize any possible impact on individuals, particularly with regards to data protection requirements.

For more information regarding the collection and subsequent processing of personal data in this context, please refer to the Data Protection Policy specific to cybersecurity-related activities.

14 Reporting cybersecurity incidents

It is essential that all Security concerns, weaknesses or incidents are reported **immediately** for examination and remedial action. The Group Cybersecurity Incident / Event notification process is published on the Group Cybersecurity Website.

Every individual working in Capgemini is required to report any observed or suspected security incident upon detection, and any potential weakness in our buildings' physical security protection, inappropriate system access, password compromises or security weaknesses in our operations or technical systems we use, that may lead to a security incident.

An incident is any event or activity which affects the ability to deliver our business or lead to unauthorized access to systems or information. Incidents may affect people, areas of the business, parts of a site, an entire site or the whole organisation depending on the nature, the extent or the cause. Incidents may be deliberate or accidental or due to a natural event, e.g. flooding. Any observed or suspected security weakness in our infrastructure, systems or services must be reported as a security concern.

Please refer to the Group Cybersecurity Incident Management and Data Breach Notification Policy for more information

When in doubt report it.

15 After you leave Capgemini

After you leave employment with Capgemini, you are still required to adhere to these duties of confidentiality. You also continue to have a duty not to disclose information to third parties or in any other way use confidential information relating to Capgemini or our clients gained during your employment with the Company.

When you leave Capgemini, you will be required to sign a declaration of personal undertaking or sign off an alternative declaration complying with local law. This will confirm your compliance (to date and in the future) with the provisions set out above regarding restrictive practices and confidential information. You must return all assets belonging to Capgemini and its client including but not limited to laptops, mobiles, authentication devices and data / Information. You must also return all Capgemini documentation given to you or compiled by you (either in physical or electronic form) during your employment regarding our business, finances, clients or delivery, so that any remaining information stored in our Assets or systems after your departure is correctly managed.
This may include copies of software, correspondence, diaries, documents, plans, specifications, drawings, company manuals, ID cards, lists of business contacts and clients, notes, memoranda, computer disks and printouts and any other documents or intellectual and industrial property.

16 Help and support

Where to look for Help / Assistance

If you are in any doubt about what to do or how to handle information i.e. how to securely transmit, store or destroy, please ensure you seek advice from a specialist.

- Your direct manager
- Your Account Manager
- Your Local Security Team
- Your BU / SBU or Global Business Line CISO
- Refer to the Group Cybersecurity Cyber Knowledge Centre
- Seek support via your IT Help Desk

17 Appendix A: Security Measures to monitor systems.

Tool	Nature / Purpose	Extent / Impact
Antivirus / Anti-malware	Antivirus and anti-malware are crucial to protecting our data and data we manage . They are designed to prevent, search for, detect and remove viruses but also adware, worms, trojans and other malicious malware.	Deployed on user endpoints and servers to detect and prevent and remove identified threats.
Endpoint Detection & Response (EDR)	Endpoint detection and response, also known as endpoint threat detection and response, is a cyber technology that continually monitors and responds to mitigate cyber threats.	Deployed on all user endpoints to detect, prevent, remove and contain identified threats.
Data Loss Prevention (DLP)	Tool used to monitor outgoing communications for the purpose of detecting potential data breaches or data ex-filtration transmissions and preventing unauthorized transmission of proprietary data].	Deployed on user endpoints to prevent unauthorized data transfer. Enforcing data leakage prevention policies.
Firewall	A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted network and an untrusted network, such as the Internet.	Deployed throughout and at the perimeter of the network. Blocking and filtering unauthorized, or potentially malicious communications.
Network Detection & Response (NDR)	Network Detection and Response is a cybersecurity solution that continuously monitors an organization's network to detect cyber threats & anomalous behavior.	Probes deployed throughout the network to detect, prevent and contain potential threats identified in network traffic.

Intrusion Prevention System (IPS)	An Intrusion Prevention System, is a technology which monitors a network for any malicious activities attempting to exploit a known vulnerability and subsequently gain access to a network.	IPS functionality can be within multiple solutions. Usually at the perimeter or egress points of a network. The solution detects and prevents known threats
Device Monitoring (User & Entity Behavior Analytics or UEBA)	User and Entity Behavior Analytics is a solution which monitors patterns of behavior on endpoints, to identify anomalies which may indicate the presence of a threat.	Centrally deployed and fed with log sources from other systems. UEBA can detect potentially suspicious patterns to be investigated.
Vulnerability Detection	Vulnerability Detection solutions, use various methods to identify potential weak points on an endpoint. These can be subsequently remediated to protect the device.	Servers, solutions and applications are scanned to identify vulnerabilities or weak points for remediations. Vulnerabilities may also be identified via penetration tests and other methods.
DNS Security	DNS Security solutions ensure the DNS security of all endpoint queries and DNS resolutions. Increase visibility into end users and devices across the network regardless of their location and blocks requests to potentially malicious sites.	Deployed on endpoints, requests to malicious external locations are blocked and prevented to protect users and endpoints.
Privilege Escalation Monitoring	Monitor and prevent suspicious escalation of privileges that may indicate potential compromise.	Deployed to fully managed user endpoints to prevent unauthorized privilege escalation.

18 Appendix B: Document Control

Author – Paul Thomas, Head of Group Cybersecurity Policy

Version History

0.1 -1.0	1/10/2018	Adoption of Cybersecurity AUP v1.0 April 2016 and revision in line with current risk profile. Further feedback from CSSO
1.1 & 1.3	7/12/2018 September 2019 Feb 2020 17/11/2020	1 - Update to Data classification name and description and Group Delivery updates 2 – Minor update, Update framework ppt with all other Policy document and completion of 2019 Policy review No content amendment to AUP Controls. Update published December 2019. 3 – Correction of administrative dates of Month on first page and footer in line with 2019 review of Policy and Mandatory Policy education program. No content amendment to AUP Controls. November 2020 – update review – no change
2.0	17/11/2020	2020 Policy review AND Published version
2.1 – 2.9	04/01/2020 – 02/03/2021	2021 Policy annual review – reviewed by Project review Board members including CSO/CISO's
3.0	03/03/2021	2021 Policy Framework - published
4.0	03/03/2022	2022 Policy Framework – Published version 2022 Policy review completed – no rule change, text update to
3.0 – 4.6	05/01/2022 – 30/11/2022	2022 Review, including Group DPO (Legel) review and contribution and Head of P&C and CCSO approval review
5.0	01/12/2022	Approved and published version

Document Distribution

Name	***Location***	***Responsibility***	***Action/ Information***
All Capgemini Employees via Group Cybersecurity Intranet Group Cybersecurity Policy Framework	Group Cybersecurity Intranet	Paul Thomas	Action/ Information

Document Reviewed By

Name	***Location***	***Responsibility***
Samir Riah	Paris, France	Group Privacy Operations Officer
Joe Morris	Atlanta, USA	Group MarCom – Social Media (including approval to Social media section)

CISO Community		CISO Community

Document Approved By

Name	***Location***	***Responsibility***
Cedric Thevenet	Paris	Group Chief Cybersecurity Officer
Edouard Zazempa	Paris	Head of Group Cybersecurity – Protection and Compliance