Information Security Policy

Capgemini Group

Edited by Group Security Committee: Bengt Ahlbin, Bjorn Gronquist, Don Coglianese, Ludovic Fiard, Cédric Laroche-Joubert , Mireille Reiners, Richard Cleaver, Markus Schuh, Sudarshan Singh

Approved by CIO Board: Bruno Nigrelli, Joshua Mc Arthur, Peter Sörensen, Theo Bouwmeister; Didier Coffin, Malcolm Porter, Jean-Christophe Lasvergnas, Valeria Toldo, Patrick Wunsch, Seshaiah Amisagadda, Pablo Quiroga Iglesias,

Reviewed by: Isabelle Roux-Chenu (Legal), Hervé Canneva (Compliance), Jeremy Roffe-Vidal (Human Resources)

Date of approval: November 2009

Version: 3 to be presented to GMB

Classification: **Company Confidential**

The information contained in this document is proprietary and company confidential. It is for Capgemini internal purposes only.

Foreword

Contributors

A special thank you to each and every contributor to this document. Beside the Group Security Committee members, the following people have helped to produce this new version of the Group Information Security Policies:

Patrick Ratel: Infrastructure Head France

Bill Millar: Director of Security OS UK

Lex Dunn: Security Officer OS BNL

James R. Farnsworth: Associate General Counsel US

Jan G. McCorstin: Chief Privacy Officer OS USA

Christian Rothhahn: Lawyer Corporate

Patrick Reijnen: Former Security Officer BNL

History

This Information Security Policy document finds its root in the very first coordinated Security Policy document elaborated by Lex Dunn in year 2001. The first edition of this document was issued in 2004 and the second edition came out in 2006. The content of the document has evolved during years to align with business needs, technology shifts and best practices. Please note that a public version of Capgemini security policy is available for clients' needs.

Bjorn Gronquist

Contents

Information Security Policy

1.1 Information Security Statement

Capgemini, Sogeti and affiliated companies, hereafter referred to as the “Capgemini Group” or the “Group”, want to protect their customers’ and their own business interests by providing a secure working environment. Proper security measures and operating procedures govern the Capgemini Group. Information Security shall be adaptive, efficient and support Capgemini Group’s business model.

- Access to information shall be controlled and based on the role of a person in the organization.
- Information security shall be aligned to the business organization and be independent of geographical locations.
- Services delivery shall be securely possible from anywhere when connected to the Capgemini Group IT Infrastructure.
- Security measures shall be consistent between countries.
- Security measures shall support the confidentiality, integrity and availability requirements of information and services.

1.2 Applicability of Policy

This Information Security Policy is mandatory within its scope of application. Capgemini Group employees, subcontractors, partners and suppliers must be aware of and comply with this policy in respect to their role when dealing with information of Capgemini Group or its customers.

Where an area of non-compliance with this policy is identified, it will be subject to risk assessment. The risk assessment will consider the possible impact of a security breach resulting from the non-compliance and the influence of any mitigating or compensating controls identified and is subject to approval from management. Local and central risk registers are maintained by the Information Security Officers.

Use of the words “must/shall/will” indicates that compliance is mandatory. Use of the words “should/may” means that compliance is expected. All deviations from this policy are subject to approval by the responsible CIO.

1.3 Scope of Policy

This document provides policies regarding Capgemini Group’s Information Security, and describes the way that confidentiality, availability and integrity are ensured. The Information Security Policy sets minimum requirements to ensure continuity and information security of global operations and is applicable to the whole Capgemini Group. Logical descriptions of security measures leave room for specific implementation and evolution in technology. Global standards and reuse of best practices will be the results of this global policy. Effective Information Security is a joint effort that requires the participation of every employee and affiliate who deals with information assets.

It is within the responsibility of the operational entities of the Capgemini Group to translate these policies into practical measures and working procedures. This policy is communicated to all Capgemini Group Business Units for application on behalf of the Group CIO.

This Information Security Policy applies to all infrastructure and information assets:

- Capgemini Group Networks, the Capgemini Group's Wide Area Networks, Local Area Networks and the Capgemini Group's telephony Networks;

- Capgemini Group personal productivity devices, servers, data storage and applications hosted at internal or external locations;

- Means of connectivity between "non-Capgemini Group" infrastructures and the Capgemini Group Global infrastructure;

- All information assets that are used for delivering the Customer and Capgemini Group services;

- Any Capgemini Group owned information where ever it is stored;

Security Policy compliance shall be monitored and audited throughout service delivery by the responsible Information Security Officer.

2. Management of Risks

2.1 Security Governance

The management of risks governs Capgemini Group's Information Security approach. Information Security is a business-enabler and is done by risk assessment at the global level. Risk. The risk-based approach ensures that proper security levels are implemented.

2.2 Risk Assessment

Potential risks are assessed to ensure the secure, continuous delivery of services to customers. Risks must be assessed for all core delivery services and all major accounts:

- By Information Security Officer yearly for Capgemini Group assets and delivery support services;
- By Risk Manager, General Counsel or Account Manager before signing the contract for major deals & accounts;
- By Project Manager when required for projects & minor accounts and approved by Information Security Officer;

Risk assessments may be conducted on any entity within Capgemini Group or an external entity that has signed a Third-Party Agreement with Capgemini. Risk assessments may be conducted on any information system including applications, servers and networks, and any process or procedure by which these systems are administered and maintained.

Risks related to security for an engagement (e.g., availability, confidentiality, integrity) using the Capgemini Group infrastructure shall be identified before the engagement starts. Security assessment shall be integrated into global risk assessments of a contract before the engagement can start.

The execution, development and implementation of remediation programs are the joint responsibility of the responsible Information Security Officer and the responsible owner for the systems being assessed.

2.3 Risk Management

Risk management is designed to limit the likelihood of a threat becoming manifest, and if so realized, managing the impact to an acceptable level. Risk treatment must come up with one of the following strategies or a combination of them:

- Avoiding the risk;
- Accepting the risk;
- Mitigating the risk to an acceptable level; or
- Transferring the risk;

Where an area of non-compliance with this policy is identified, it will be subject to a risk assessment. All exemptions must be approved by the responsible Business Unit CIO. All exceptions must be reported to the Group Security Committee and recorded in the risk register.

3. Security Organization and Procedures

The following security organizations and procedures will be implemented.

3.1 Security Organizations

The **Chief Information Officers** (CIOs) of the operational entities within the Capgemini Group have responsibility for Information Security within their respective entities. The Chief Information Officers have delegated planning, execution and follow-up of security tasks to their Information Security Officers.

The **Group Security Committee** is composed of Information Security Officers from Major Business Units and the Group Security Committee Chair who participates in the Group CIO Council.

The **Group Operational Security Council** is composed of Information Security Officers from all operational units and the Group Security Committee Chair. It reports back to the CIO Council.

The Group CIO Council

- approves the security policies and procedures proposed by the Group Security Committee;
- is responsible for the implementation of approved security policies and procedures.

The Group Security Committee

- develops and maintains the Capgemini Group security policies, standards and procedures;
- audits the implementation of policies, standards and procedures throughout the Group and
- supports continuous improvement of overall information security.

Information Security Officers

- are responsible for maintaining, developing and promoting the enforcement of security policies, standards, guidelines and procedures in their respective entities;
- are responsible for auditing implementation of policies, standards and procedures throughout their respective entities;
- handle security incidents within their respective entities and
- shall manage security within their operational entity and hold regular meetings.

The Operational Security Council

- is responsible for the overall security governance;
- is the body to which Information Security Officers report all security related topics of their operational entities on a bi-monthly basis;
- is responsible for managing security incidents of Level 1 or 2 (see Section 10.1);
- identifies information security-responsible individuals at the beginning of each year for all operational entities.

The Security Forums

- should be created at the appropriate levels of the Capgemini Group's organization to coordinate security topics with shared responsibility;
- should organize regular meetings that include at least the following business parties:
  - Facilities, Human Resources, Legal, IT, Business Risk Management and Privacy Departments;
- should regularly discuss and decide on security aspects regarding information security related to compliance, security-related incidents and Information Security Awareness.

3.2 Information Security Framework

Security policies lay out the security principles, rules and standards to which everyone must conform. They set out the rationale for the protection needed for the Capgemini Group. The

Capgemini Group Security Policy Framework, as described below, helps users and providers of information and services understand their responsibility and accountability.

Security documents are issued at three levels:

Group Level: Security documents at this level apply to all organizational units. All statements have to be considered as minimal requirement and must only be enforced by any other level policies (if existing). Group level documents ensure consistent delivery and performance within the Capgemini Group. These documents are issued by the Group Security Committee and approved by the CIO council.

Business Unit level: Security documents at this level apply to the Business Unit. They have to be compliant with Group-level documents. These documents are reviewed by the responsible Information Security Officer for the Business Unit and approved by the Business Unit CIO.

Specific Unit level: Security documents at this level apply to the specific operational entity within a business unit. They are reviewed and approved by the responsible Information Security Officer for the Specific Unit and must be in line with group and business unit policies.

4. Asset Management

4.1 Assets

The Capgemini Group must protect all assets needed for its business operations and which, directly or indirectly, support information processing. All critical assets must be identified and the responsible owner must be clearly defined. These assets are classified in the following categories:

- **Information Assets:** this is the actual data and information that is owned by, shared and used within the Capgemini Group, its Customers and third-parties;
- **Software:** these are business applications hosting and processing information and applications and code providing supportive functions like operating systems;
- **Physical Assets:** these are the actual physical resources such as servers, workstations, printers and buildings etc.;
- **Services:** Services on which computer systems depend: computing and communications services, intrusion detection devices and general utilities such as heating, lighting, power and air conditioning;
- **Human resources:** these are persons that are ensuring services for Capgemini Group and its Customers;
- **Intangible assets:** Assets other than tangible assets such as reputation, goodwill, intellectual property and brand image etc.

4.2 Classification of Assets

Information Assets must be classified appropriately (Public, Company Confidential, Customer Confidential & Sensitive Information) in order to ensure that information receives an appropriate level of protection. If an asset is not classified by the owner then it will be classified as “Company Confidential” by default. Appropriate security measures must be applied based on the information classification.

- **Public Information**:
  This information is intended to be publicly available. Information made public on behalf of the Capgemini Group must be approved prior to being published. Documents must be properly protected to guarantee their integrity.
  - This information is intended for use in the public domain.
  - There is no authentication or authorization controls required for this type of information.
  - The Capgemini Group information shared as Public Information will be protected against common security threats and vulnerabilities in the public domain.
  - The information integrity must be protected.

- **Company Confidential:**
  This Information category is the default classification for all Capgemini Group owned and managed information. All information shall be considered as Company Confidential unless stated otherwise.
  - This information is intended to be regular business information.
  - This information is only intended to be available to all Capgemini Group employees and specifically authorized third-parties for use in the performance of services for or on behalf of the Capgemini Group.
  - Authentication and authorization controls must be in place.
  - This information will be protected for common security threats and vulnerabilities.
  - The information integrity, availability and confidentiality must be protected.

- **Customer Confidential:**
  Customer Confidential information should only be shared with people involved in the specific engagement that have the need to know. This information may be covered by Non-Disclosure Agreements. The Capgemini Group may be held responsible if such information is divulgated.
  - This information is only available on a need-to-know basis for authorized Capgemini Group employees and specifically authorized subcontractors.
  - Authentication and Authorization controls must be in place.
  - This information will be protected for common security threats and vulnerabilities.
  - The information integrity, availability and confidentiality must be protected.

- **Sensitive Information:**
  This is highly confidential information that could damage the interests of the Capgemini Group or of the party to whom the information belongs if in-appropriately disclosed:

- This information is only for specified recipients.
- This information is only available on a need-to-know basis to a limited group of persons in the performance of services
- Authentication and authorization controls must be in place.
- This information must be protected for common security threats and vulnerabilities.
- The information integrity, availability and confidentiality must be protected.

5. Human Resources Security

5.1 Security Awareness

All Information Security Officers shall ensure that employees, contractors and third-party users are aware of information security threats and concerns, their responsibilities and liabilities, the relevant Capgemini Group policies and are equipped to support information security in the course of their normal work, and to reduce the risk of human error. Therefore Information Security Officers must:

- ensure that their employees, contractors and other parties doing business with them, have the appropriate level of security awareness;
- set up targeted awareness programs for all employees, contractors and third parties whenever this is required for assignments or any other situation that occurs;
- carry out overall awareness programs for all employees, subcontractors, partners and suppliers on a regular basis;
- make sure that contractors and third-party users have signed Non-Disclosure Agreements that fit their working situation;
- make sure that the employees ,contractors and third-party users report any security incidents;
- make sure that employees and subcontractors are aware of the obligation to return all assets on termination of their engagement.

5.2 Publishing and Social Networking

While Capgemini Group employees are allowed and even encouraged to publish in paper or electronically in blogs, news sites and social networks, publishing is subject to the Capgemini Group's rules and regulations:

- Publishing and social networking must be done in a professional and responsible manner,
- Public statements about Capgemini Group and Capgemini Group's vision must be approved by Corporate Communication**.**

- Publications and social networking must not be detrimental to the Capgemini Group's , its customer's and third-parties' interests, and shall not interfere with any employee's regular work duties.

- The Capgemini Group's or its customer's confidential or proprietary information, trade secrets or any other material covered by the Capgemini Group's or its customer's confidentiality policies must not be revealed.

5.3 Privacy Policy

Personal Information shall mean any information relating to an identified or identifiable natural person. It includes but is not limited to name(s), address, contact details, identification numbers, factors specific to his/her physical, physiological, mental, economic, cultural, or social identity. The Capgemini Group understands the importance of protecting the privacy of its current, former and prospective employees, third-parties and customers and endeavors to run its business in compliance with applicable data protection laws and regulations. To that end, the Capgemini Group will endeavor to:

- take reasonable steps to respect the Privacy and the Personal Information of their current former and prospective employees, third-parties and customers***;***
- collect, process, store and transfer Personal Information in compliance with applicable laws and regulations;
- not sell or trade Personal Information to other parties;
- only disclose Personal Information on "a need-to-know" basis for performance of work;
- classify Personal Information as Sensitive Information;
- require its employees and contractors to abide by their confidentiality obligations;
- employ physical, electronic, logical and organizational safeguards and procedures designed to protect the confidentiality, security, and integrity of Personal Information;
- notify the client, as permitted by laws, of any request for disclosure of Client Personal Information by a law enforcement authority;
- notify the client, as required by laws or contract, if the security, confidentiality or integrity of the unencrypted Client Personal Information is compromised where it is aware of such compromise;
- deal properly with all inquiries from Clients relating to Capgemini Group's processing of transferred Client Personal Information according to mutually agreed upon terms.

6. Physical and Environmental Security

To prevent unauthorized physical access, damage and interference to the Capgemini Group's premises and information, The Capgemini Group shall implement measures and controls outlined in the following paragraphs.

6.1 Buildings

- The access to the Capgemini Group buildings must be sufficiently controlled.
- Visitors shall only have restricted access to Capgemini Group buildings.

6.2 Data Centers

The Group Security Committee maintains a list of official data centers and audits their compliance toward this policy.

- Data centers must be secured to be accessible to only authorized employees.
- Visitors must be supervised by an authorized employee when accessing the data centers.
- Entry of and departure from the data centers must be recorded and kept for 6 months.
- Access rights must be regularly reviewed and updated, and revoked when necessary.
- Data centers must have appropriate environmental control for the equipment, e.g., power, air conditioning etc.
- Video monitoring and intruder detection may be in place

6.3 Computer Rooms

- Access to computer rooms must be secured to restrict access to only authorized employees and subcontractors.
- Access from public or open areas should not be possible.
- Entry of and departure from the computer rooms should be recorded and kept for 6 months.
- Access rights shall be regularly reviewed, updated and revoked when necessary.
- Visitors must be supervised by an authorized employee when accessing the computer rooms.

6.4 Infrastructure Equipment

- Infrastructure components like servers, network switches and storage components must only be placed in computer rooms or data centers.

7. Communications and Operations Management

7.1 Communications

All applicable policies standards and guidelines must be published and communicated to relevant persons.

All changes to policies, standards and guidelines shall be announced through regular processes to relevant persons.

7.2 Operations Management

To ensure the correct and secure operation of information processing facilities, operating procedures must be documented, maintained, and made available to relevant users.

- Responsibilities and procedures for the management and operation of all information processing facilities must be established.
- Appropriate operating procedures must be documented and maintained.
- Segregation of duties should be implemented to reduce the risk of system misuse.

8. Access Control

Major assets within the Capgemini Group are the information assets supported by the global infrastructure and application systems. These assets require protection from unauthorized access and possible abuse.

Access control provides protection for information assets based on their classification by using the concept of network zones in combination with authentication and authorization.

8.1 Access and Identity Management

- User registration
    - All Capgemini Group employees and subcontractors must be registered in the Corporate Directory. Subcontractors' access must be limited to 6 months and be renewed, if required.
    - All external users including partners and customers requiring access to non-public information must be approved by a Capgemini Group employee and must be registered in the Corporate Directory. Access must be limited to 6 months and be renewed, if required.
    - All users, third-parties, subcontractors, and employees that no longer need access to the Capgemini Group's information assets must be disabled in the Corporate Directory and in any applications or systems having their own user management processes within a maximum of 48 hours after notification. User registrations must be removed from the Corporate Directory and any other systems within 6 months.
    - Each operational entity is responsible for the registration and management of its users.
- User identification & access
    - Access to information and services must be restricted, controlled and provided only after successful identification and credential checking in the Corporate Directory or a directory approved by the security committee.
    - All users must use personal identifiers based on the Corporate Directory to access any information systems.
    - Whenever possible applications shall use the corporate single sign on for authentication.

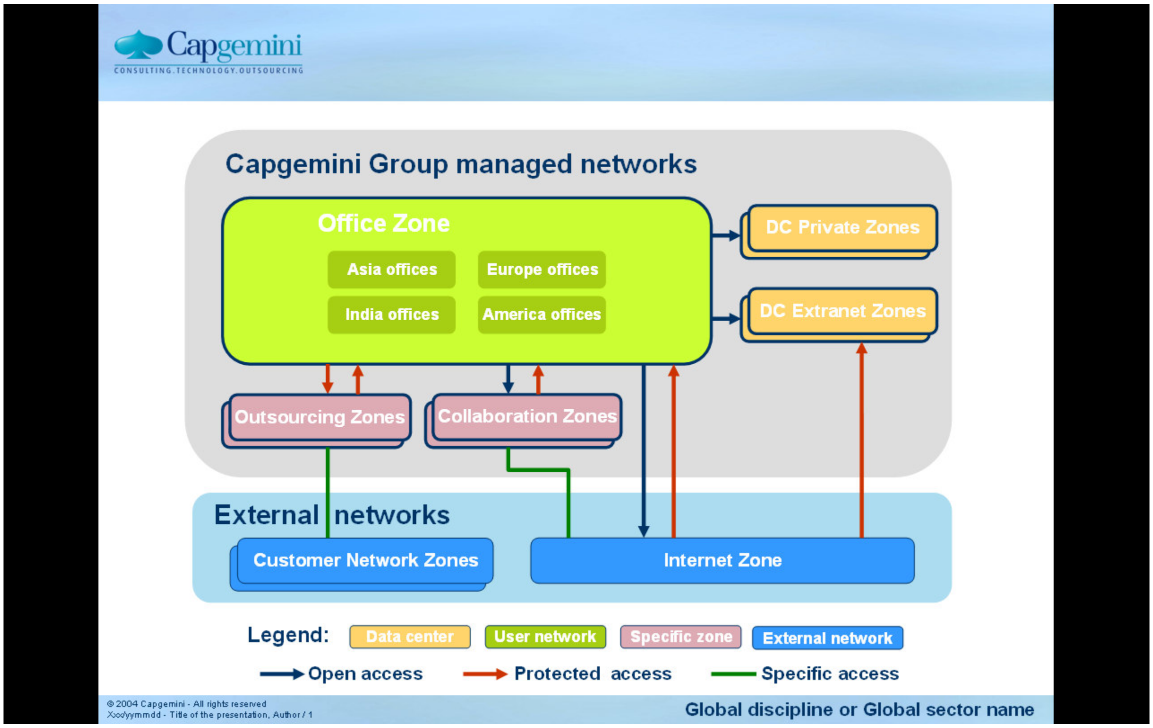
  - Users must not share any personal credentials, whether weak or strong, with others for providing access.
  - Administrative access to systems must be logged so that transactions can be related to an identified user.

- Password management
  - All user accounts must have a password.
  - All passwords must be at least 8 characters long.
  - Passwords must be changed at least every 3 months.
  - Administrators and helpdesks must provide personalized passwords to users. Password generator tools shall be used.
  - Passwords allocated by service desks must be changed on first login.
  - Password history must be maintained for at least 3 previous passwords.

8.2 Network Access

The Capgemini Group prevents unauthorized access and abuse of networks in order to protect the Capgemini's and their customer's systems. To meet this objective the Capgemini Group's network is segregated into different network zones, each having their own means for use and appropriate access control. Access to network zones and systems within the Capgemini Group is only provided on a "need-to" basis.

The following scheme shows the different network zones and their access control.



Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

Capgemini Group managed networks

Office Zone

Asia offices

Europe offices

India offices

America offices

DC Private Zones

DC Extranet Zones

Outsourcing Zones

Collaboration Zones

External networks

Customer Network Zones

Internet Zone

Legend: Data center · User network · Specific zone · External network

→ Open access · → Protected access · — Specific access

© 2004 Capgemini - All rights reserved
Xxx/yymmdd - Title of the presentation, Author / 1

Global discipline or Global sector name

Zone	Definition	Confidentiality & Access	Availability & Audit
Office Zone	This is the major network zone to which user's notebooks desktops and office tools (printers, faxes, etc.) are connected. The Office Zone covers all buildings over the world where Capgemini Group users are located. All offices are transparently connected over the Group's global network into one logical zone. Therefore a user working in other Capgemini Group offices shall not notice any differences in access to his/her service.	All information within this zone is by default classified as Company Confidential. Access to this zone is only possible from: • a Capgemini Group building with physical access protection. • external networks only after strong authentication and with encrypted connection through approved corporate access points. Once connected, users devices are part of the Office Zone. Access to office systems in this zone shall be protected with personalized user IDs and passwords.	Availability of Office Zone networks must be maximized. All unsuccessful access attempts should be logged and kept for 12 months.
DC Private Zone	This zone is aimed at hosting Capgemini Group's internal business applications that shall be available from anywhere in the Office Zone. Examples are Group applications such as Talent and KM2 and local applications such as Intranets.	Information in this zone is classified as Company Confidential. This zone must be hosted in a data center or computer room and access must be protected by a firewall. Access to this zone: • Services can only be accessed from the Office Zone or through approved access devices after proper authentication. • Access to business services must be protected with personalized user IDs and passwords. • Authorization must be based on personal roles.	Availability of services is determined by a business continuity plan and managed with SLA's. Incidents are handled in conformance with DR-plans. Access to services should be logged and are kept for 12 months.
DC Extranet Zone	This zone hosts Capgemini Group systems that need to be accessible	Information in this zone may be classified as Public Information,	Availability of services is

	both from the Office Zone and from uncontrolled networks such as the Internet. DC Extranet net Zone hosts applications which Capgemini Group shares with its Customers. Examples are troom-x, coconet	Company Confidential or Customer Confidential Information. Information classified as Sensitive Information must not be stored in this zone. Access to this zone is possible: • from the Capgemini Group offices. • from external networks when encryption and appropriated authentication is used. • Public information may be provided without authentication or encryption. • Systems must be protected against unauthorized access.	determined by a business continuity plan and managed with SLA's. Incidents are handled in conformance with DR-plans. Access to services should be logged and kept for 12 months.
Collaboration Zone	This zone is hosting project servers, development systems and eventually workstations. This zone can have connections to any Internet zone in a controlled manner. Capgemini Group and external persons (customers or partners) can work together on projects in this zone. A typical Collaboration Zone is the Accelerated Development Centre (ADC). This zone can be connected with a client network.	All information in this zone is classified by default as Company Confidential. Proper Information classification and protection must be provided by the information owner. Access to: • Access is granted from the Office Zone and can be allowed from external networks. • Access to this zone and hosted systems must be protected with (weak) authentication. • However Encryption and strong authentication are recommended. Systems must be protected against unauthorized access. Users located in a Collaboration Zone can only access the Office Zone through authorized access devices.	Availability of services is determined by a business continuity plan and managed with SLA's. Incidents are handled in conformance with DR-plans. Access to services coming from non-Capgemini Group networks should be logged and kept for 12 months
Outsourcing Zone	This zone hosts systems operated by the Capgemini Group on behalf of its customers.	All information in the Outsourcing zone is classified as Customer Confidential.	Availability must be managed in conformance with SLA's defined

	This zone should not contain any end-user devices. Access to this zone must be restricted to authorized employees of the Capgemini Group. Systems in this zone may be accessed from customer networks. Outsourcing Zones are protected in accordance with the needs of the customer.	Access: • Capgemini Group employee access to an Outsourcing Zone should be protected with strong authentication. • Authorizations are based on personal roles and proper authentication.	between OS and customer Access to services is logged and should be kept for 12 months.
Internet Zone	This zone is in fact any zone which is not under control of the Capgemini Group and not identifiable as a specific Customer Network Home offices, public Internet access points, partner networks and other networks not directly connected to the Capgemini Group network are considered as Internet zones.	Classification: No confidentiality can be guaranteed in this zone. All information residing in this zone is assumed to be classified as Public Information.	No availability can be guaranteed by the Capgemini Group.
Customer Network Zone	This zone is managed by a Capgemini Group customer or partner. The zone may be connected back to an Outsourcing zone via a dedicated network connection. This zone is the customer's network that may be granted access to an Outsourcing Zone.	Access: Access to Customer Network Zones must be protected to limit possible damage.	Availability is managed by the customer.

8.3 Mobile and Remote Access

- Remote access shall only be allowed when using approved Capgemini Group access services.
- Remote access to the Capgemini Group services must be based on encryption and approved strong authentication.
- **All** mobile networks must be considered as remote access networks.
- Remote access policies must apply to Wireless LANs.

9. Information Systems Acquisition, Development & Maintenance

The design and implementation of the information system supporting the business process is crucial for security. Security requirements must be identified and agreed upon prior to the development and/or implementation of information systems.

9.1 General Data Protection

To prevent errors, loss, unauthorized modification or misuse of information in applications, appropriate controls should be designed into applications, including user-developed applications to ensure accurate processing. These controls should include the validation of input data, internal processing and output data. Additional controls may be required for systems that process, or have an impact on, Sensitive Information.

- All non-public information stored outside of the Capgemini Group premises should be encrypted or be kept in a secure environment.
- All Sensitive Information must be encrypted when stored or transmitted outside the Capgemini Group's premises.
- All Sensitive Information should be encrypted when stored or transmitted inside the Capgemini Group's premises.
- All information stored on Capgemini Group systems or media must be destroyed when media are taken out of service (paper documents must be destroyed by shredding, electronic media by degaussing or destroying the media itself).
- Sensitive Information, Company Confidential and Customer Confidential Information must only be stored on external sites after formal approval of the CIOs.

9.2 Application Security

System software, projects and support environments must be strictly controlled in order to maintain the security of applications. Managers responsible for applications should also be responsible for the security of the project and the support environment. They should ensure that system configurations are hardened and that all system changes are reviewed to check that they do not compromise security of either the system or the operating environment.

Email

Incoming and Outgoing email traffic must be scanned for viruses, spam and other malware.

Incoming spam should be centrally quarantined with the possibility for the employee to access his/her quarantined email.

Virus and anti-spam definitions on the email servers & gateways should be updated as soon as possible after they are released by the vendor.

Automatic forwarding of the Capgemini Group emails to non-Capgemini Group mailboxes must not be implemented.

Public Collaboration Tools

Instant messaging with parties inside or outside the Capgemini Group network should be centrally-managed and use secured IM gateways that are under control of the Capgemini Group.

All employees must be made aware of the risk associated with public instant messaging.

Gateways should be able to filter messages based on content, force encryption and block transfer of files.

Corporate Domain Controllers

Domain controllers should be hosted in a private zone or protected properly when hosted in an office zone.

All Capgemini Group Active Directories must never trust other Active Directories.

Web Applications

Web applications must be properly tested and maintained against security threats.

Non-Web Applications

Strong authenticated and encrypted connections must be used to access non web-based applications from outside of the Office Zone.

9.3 Project Control

To ensure that security is an integral part of information systems, all security requirements must be identified at the requirements phase of a project and justified, agreed, and documented. Information systems include operating systems, infrastructure, business applications, off-the-shelf products, services, and user-developed applications.

- Access to system files and program source code should be controlled.
- IT projects and support activities must be conducted in a secure manner.
- Care must be taken to avoid exposure of Customer, Company Confidential and Sensitive Information from test environments.
- Using production data in test environments without production level controls should not be allowed.

9.4 Encryption & Certificates

Encryption

Safe, efficient and effective deployment of cryptographic services is defined in this section.

- The generation of cryptographic keys or other elements input into algorithms must be secure.
- The use of a key, in terms of time in use must be limited to avoid crypto-analysis or brute force key cracking.
- When requested by law enforcement agencies or legislation, a process to recover encrypted data must be put in place.
- Encryption should protect the laptops, mobile devices & applications on these devices with Company, Customer Confidential and Sensitive Information.
- Use of cryptographic technology must be in compliance with local legal requirements.
- Users visiting other countries should make themselves aware of specific encryption technology laws.

Certificates

- The Capgemini Group allows the use of two types of certificates:
    - External recognized certificates provided by recognized certification entities.
    - Internal recognized certificates provided by the Capgemini Group certification entities validated by the security committee.
- Internal certificates should be used whenever possible. External certificates shall only be used when external recognition is required by business.
- Internal certificates must only be delivered for users and devices registered in the Corporate Directory or a directory approved by the Security Committee.
- Only the Capgemini Group user certificates and computer certificates must be used for securing Infrastructure services when accessed from personal productivity tools.
- The use of internal certificates in communication with external party shall only occur after formal approval of the Capgemini Group internal certification entities by the party. All other use of internal certificates with external partners shall be avoided.
- Certificates together with weak (password) authentication is considered as two-factor authentication.

9.5 Personal Communication Devices

- Personal communication devices (PCDs) shall be protected before being granted access to the Capgemini Group network & or services.
- Employee-owned PCDs can be used for the Capgemini Group business only when approved by the responsible CIO.

- Files containing Company Confidential, Customer Confidential and/or Sensitive Information should not be stored in PCDs unless protected by encryption and password.
- All connections to the Capgemini Group network and services must use two-factor authentication and encryption for communication.
- Lost or stolen equipment used for the Capgemini Group Information assets must immediately be reported through the proper channels.

10. Incident Management

10.1 Incident Handling

- Responsibilities and procedures must be in place in all operational entities to handle information security events.
- Evidence for security incidents should be collected to ensure compliance with legal requirements.
- Information security events and weaknesses associated with information systems must be communicated in a manner allowing timely corrective action to be taken.
- Formal event reporting and escalation procedures must be in place. If an event involves potential disclosure of non-public personal information, then the Office of General Counsel and Privacy Officer should be notified and involved in the incident management process.
- All employees, contractors and third party users must be made aware of the procedures for reporting incidents.
- All security incidents must be reported to the local service desks and, if the impact is outside of local responsibility, to the Global Command Center and initiate escalation processes when required.
- Escalation path is:
    - Information Security Officer of operational entity.
    - Business Unit CIO and Security Committee.
    - Business Unit CEO and Group CIO.
- The Global Command Center must be involved for all incidents impacting more than one security area and coordinate resolution.
- All incidents must be classified into the following 5 levels:
    1. major business impact;
    2. medium business impact;
    3. limited business impact;
    4. increased alert level:

5. normal operation.

- For major and medium incidents the Operational Security Council head will take the lead and the CIOs shall be ultimately responsible for taking the appropriate decisions.
- All security incidents must be reported in the operational security reports.

10.2 Improvement Process

- The organization shall take corrective actions to eliminate the root cause of incidents.
- Preventive actions shall be reported to the Operational Security Council.

11. Business Continuity Management

Proper measures should be in place to provide the right level of availability of all Information Services. These measures are based on the assessment of business risks and cost. The measures should be in relation to the current situation and criticality of the systems.

- All components which are critical to the operation of the Capgemini Group IT infrastructure must provide high availability.
- Business continuity plans must exist and should be tested at least every year, for all critical parts of the Capgemini Group delivery framework.
- Adequate measures will be in place to backup critical data and to ensure information protection.

12. Compliance

12.1 Software

- For all software used within the Capgemini Group software licensing must be in place and regular auditing should be done.

12.2 Audits

- The implementation of these Information Security Policies should be audited by the Group Security Committee every year within the scope of the Capgemini Group.
- Results must be communicated to the CIOs who are responsible for taking the appropriate measures to adjust operations in case of any deviation from the Global Information Security Policy.
- Corrective and Preventive Action Plans should be followed up by the responsible Information Security Officer and communicated to the Global Security Council on a bi-monthly basis.

- New entities, acquired by the Capgemini Group, should be audited and their integration into the Capgemini Group core infrastructure should only be allowed after risk assessment is approved by the responsible CIO and mitigating measures are in place.
- Responsible security entities must be granted right to audit all assets before being put into service.
- Appropriate procedures shall be implemented to ensure the respect of intellectual Property Rights, and the use of proprietary software products.

12.3 Enhancements to Compliance

- The Group Security Committee shall review the Capgemini Group's information security management system (ISMS) on a regular basis but at least every year to ensure its continuing suitability, adequacy and effectiveness. This review shall include assessing opportunities for improvement and the need for changes.
- The Group Security Committee shall identify changed risks and identify preventive action requirements. The priority of preventive actions shall be based on the results of the risk assessment.

12.4 Information Retention

- The Capgemini Group must comply with local laws and regulations on information retention in particular for HR, legal and financial applications.
- Information owners must ensure that information assets are legible, stored and can be retrieved for audit and analysis.
- Third-parties will be requested to retain information in accordance with the Capgemini Group's and its customer's needs.
- Obsolete information assets will be identified and destroyed with the agreement of the information owner and the customer.

13. Terminology

Corporate Directory refers to the Capgemini Group's central directory providing authentication and authorization services for access to applications, Capgemini's Intranet and to network services. The Corporate Directory is updated from HR systems. It provides white and yellow pages information.

Information Security Officer is the responsible for information security management in an operational entity.

Group refers to the highest level of Group operations headed by the Capgemini Group CEO.

Business Unit refers to an operational unit reporting directly back to the Group CEO.

Specific Unit can be any clearly identified entity within the Capgemini Group.

Group Security Committee is the Capgemini Group's security body. It is the Guardian of proper Information Security implementation.

Global Command Center is the Capgemini Group's central support service responsible for supervising all global services and handling all global incidents.

14. References

- ISO/IEC27001:2005 – Information Security Management System Requirements
- ISO/IEC27002:2005 – Code of Practice for Information Security Management
- ISO/IEC27005:2008 – Information Risk Management
- The Capgemini Group's Blue Book