GRENOBLE
ECOLE DE
MANAGEMENT
BUSINESS LAB FOR SOCIETY

une école
CCI GRENOBLE

Guidelines on using the resources in the Information and Communication System

Audience:

GEM Learners

CONTENTS

Foreword

Grenoble Ecole de Management (GEM) defines, deploys, maintains and operates an Information and Communication System (*ICS*) as required to perform its activities. The *ICS* comprises various hardware, software and documentary *Resources*, including a number of servers, *Workstations* and services that exchange information over IT and telephone networks.

As part of GEM's policy for transparency and its determination to encourage *ICS Users* to use the information system in a fair, responsible and secure manner, these Guidelines set forth the terms and rules for using *ICS Resources* and define Users' associated rights and obligations.

These Guidelines may be supplemented by *Documents* that apply to specific categories of *Learners*.

The IS Division (*ISD*) also provides *Users* with additional best practice guides, which describe the specific uses and applications of the hardware and software available, along with their organizational and technical environments.

The *ISD* welcomes enquiries and questions from all *Users* when applying these Guidelines.

These Guidelines are attached to the Study Regulation and are brought to the attention of the *Users* at the moment of their enrollment.

1. Definitions

A. Glossary

A glossary is appended to give readers a clearer understanding of these Guidelines. This glossary defines all the technical terms and especially the computing terminology used in these Guidelines.

B. Reserved keywords

The following keywords provide an accurate and unambiguous definition of the different levels of requirements featured in these Guidelines, so that all *Users* of the GEM *ICS* can clearly understand their authorizations and options during their daily or occasional use of the *Resources* available.

The keywords "must", "shall", "must not", "shall not", and "may" have the following meanings:

- "Must" and "shall": these terms convey an absolute obligation. If one or more exceptions are available, they are explicitly and exhaustively described in these Guidelines.
- "Must not" and "shall not": these terms mean that something is strictly forbidden. If one or more exceptions are available, they are explicitly and exhaustively described in these Guidelines.
- "May": this term describes an optional use or indicates an exception to an obligation or a forbidden action.

For any questions concerning the use of a specific *ICS Resource*, *Users* are invited to contact the School Department or the *ISD* for further clarification, so that they can use the Resource in both an effective and secure manner.

2. Scope of these Guidelines

A. Users concerned

These Guidelines apply to *Users* of the GEM *ICS* such as defined in the appended Glossary. They concern *Learners*: people who come to take an initial or continuing training course at GEM.

B. Information and communication system (ICS)

The *ICS* contains, organizes and manages all the authorized communication and IT resources, such as defined in the foreword and which can be used on GEM premises or remotely, including web services. These web services use local or offsite servers to provide various means for sending and exchanging information, such as websites, collaborative workspaces, email and instant messaging, chat rooms and social networks.

By extension, it contains all the digital data that are stored, processed and exchanged by these mechanisms.

3. Access to ICS Resources

The components of the GEM *ICS* are and will continue to be GEM's property, excluding the *Users*' personal *Hardware* employed for the needs of their training course. Any such usage is authorized by default in GEM *ICS*, provided that all of the clauses in these Guidelines are complied with strictly and in full.

The *ICS* is made available to the *Users* by the *ISD* for educational and information purposes exclusively. In addition, the extent of the *ICS Resources* to which the Users have access may be limited on the basis of the actual needs and of the constraints imposed by sharing these *Resources* with other *Users*.

The *ICS* is made available under the conditions defined during the *User*'s enrollment at GEM, until the course comes to an end, with the award of a qualification (diploma or certificate), a training attestation, or the interruption of the course before obtaining a qualification or attestation.

The right of access is temporary. It is withdrawn if it is no longer justified by the *User*'s status. It may also be withdrawn as a protective measure if the *User*'s behavior or use of the *ICS* no longer comply with the rules set out in these Guidelines.

A. User account and connection settings

User access to *ICS Resources* is subject to the creation of a *User Account* by the *ISD*. The *ICS* access rights for this account are managed by the *ISD*: they change in line with educational needs and are then progressively withdrawn after the end of the *User*'s training .This progressive withdrawal conforms to the calendar defined for the course being taken.

The *ICS* is accessed and used, by default, from a private individual *Workstation*. The use of collective *Workstations*, made available and specifically configured by the *ISD*, will be mandatory for certain educational purposes, which will be expressly stipulated.

For particular individual needs, the *ISD* provides a *Workstation* under a contractual loan agreement.

Finally, shared self-service *Workstations* are made available by GEM to provide a range of services such as the printing of documents.

The rules and conditions for the use of individual or collective *Workstations*, whether private or provided by GEM, for access to the *ICS*, are described in Section 5A of these Guidelines.

Users must comply with all the rules in these Guidelines to help maintain the performance and *Security* of any *Workstation* that they are duly authorized to use for the furtherance of their training. The vast majority of *Workstations* are mobile, so Users shall exercise special care and attention according to the provisions of Section 5A in these Guidelines. All *Users* of a collective *Workstation* must abide by the rules in these Guidelines that strictly apply as with any individual *Workstation*.

Access to certain components of the *ICS* is protected by connection settings (username, password, digital certificate, etc.), which must fulfill the specific *Security* criteria defined by GEM.

Connection settings are strictly personal to the *User*. *User* shall commit their settings to memory and maintain their confidentiality. They must not be disclosed to third parties, written down, printed out or stored in an unsecure manner either inside or outside the *ICS*.

Where connection settings are chosen by the *User*, they must meet specific complexity requirements and must be changed at regular intervals. Therefore, *Users* must observe the *Security* instructions implemented and disseminated by the *ISD*.

In addition, *Users* must not use an account belonging to another *User*.

B. Authorized uses

ICS Resources are primarily used to fulfill the needs of GEM's activities. *Resources* are chosen, configured and sized to achieve this professional objective.

Therefore, *Users* shall prioritize use of these *Resources* when performing their training activities at GEM in accordance with applicable rules and the provisions of these Guidelines.

Resources may be used for personal or private purposes, provided that such use is reasonable in terms of quantity and duration, meaning that it does not affect the *Security* or performance of the *ICS*.

Section 5 in these Guidelines features a detailed description of the mandatory, recommended or optional best practices for the *User's* training needs and the permitted uses for personal or private purposes.

C. Computing hardware made available

Each GEM Campus can provide *Users* with self-service *Hardware* devices or individual *Hardware* devices under a contractual loan agreement.

To maintain self-service equipment in good working order, *Users* undertake to:

- Comply with the instructions in these Guidelines
- Close the session opened with their *User Account*
- Leave a clean and tidy space in the *Workstation* environment after use
- Inform the *ISD* of any *Hardware* malfunction or breakage

❖ Behavior in rooms with self-service Hardware

Users must not eat or drink while using one of the *Hardware* devices made available.

So that everyone can work in peace and quiet, mobile devices such as telephones and tablets must be turned off at all times when in rooms equipped with computers (computer rooms, Resource Center, or other facility), unless expressly authorized by a member of the teaching staff or other accredited GEM personnel.

Users must leave the workspaces they use clean and tidy when they have finished.

4. *ICS* protection and security rules

GEM uses its best efforts to provide the necessary manpower and technologies to maintain the *Security* of the *ICS*. As such, it controls access to the *ICS* and acquires the intellectual property rights or obtains the necessary authorizations to use the *Resources* made available to *Users*.

A. Duties of ICS Users

Users are responsible for the *Resources* entrusted and which they use for the purposes of the attended training. They agree to exercise caution, vigilance and fairness when using *Resources* and also take the necessary precautions to help maintain the *Security* of the *ICS*.

Users shall not perform any activities that are unlawful or likely to harm GEM's interests.

Users shall not give other *Users* or unauthorized people access to the *ICS* in any way whatsoever.

When leaving their private *Hardware*, even temporarily, *Users* shall lock access when the *Workstation* is no longer within their direct field of vision and when *Users* have an active work session under their

User Account on that *Workstation*. *Users* must always keep in their possession any external identification and/or authentication *Hardware* devices that have been allocated to ensure their access to an *ICS Resource*.

With regard to self-service *Hardware* or *Hardware* on individual loan, *Users* shall not:

- Disable the automatic locking mechanisms set up by the *ISD*.
- Install any *Hardware* or *Software* without the prior consent of the *ISD*. Installation must be explicitly performed by *ISD Personnel*.

They shall not copy any *Illegal Files* or files that are contrary to public order or likely to harm GEM's image.

Users shall not circumvent the usage restrictions on the *Software* or perform any actions that are likely to modify or destroy the property, services and *Resources* of the *ICS*.

Users shall record the data files that they create, modify, copy or receive exclusively on a fixed or removable storage *Resource* on their individual *Workstation* or on *ICS Resources* explicitly authorized by the *ISD* such as their individual *Cloud Drive*.

Users shall not copy the data onto other *Resources* that have not been authorized by the *ISD*.

Users shall not access *ICS Resources* for which they have not received explicit authorization. In particular, they shall not read the information held by other *Users* and for which they know that access is forbidden. For example, *Users* shall not access personal or private conversations for which they are not a recipient, whether direct or copied in.

5. Terms for using ICS Resources

A. Hardware, software and services

Users utilize their private *Workstations*, but these must be configured before the first connection to the *ICS*, in order to comply strictly with the security requirements defined by the *ISD*. The *ISD* reserves the right to refuse access to the *ICS* from any particular *Workstation* in order to maintain the *Security* and performance of the *ICS*. In case of mobile *Hardware*, such as a laptop, tablet or smartphone, *Users* must sign a loan form defining the terms for using the *Hardware*.

Users shall apply, and comply strictly with, the configuration recommendations presented to them at the time of enrollment.

To benefit fully from the *ICS Resources*, *Users* can check with the *ISD* that their private *Hardware* complies with the following rules:

- Any *Software* installed and used for educational activities must be up to date, including the operating system or systems that enable the said *Software* to be run.
- For all *Software* installed on their private *Hardware*, *Users* must be able to prove that they hold a user license allowing them to use it in the context of their training at GEM.
- All private *Hardware* must be equipped with *Software* for protection against the *Download*, installation and execution of any malicious software code. The protective software in question must be authorized by the *ISD*, must be constantly operational, and must be kept up to date in accordance with its editeditor's update policy.
- The use of private *Hardware* devices within GEM must under no circumstances disrupt the training courses dispensed or impede GEM's activity.

Users may access the GEM *ICS* remotely using a loaned and/or authorized private *Hardware* device, subject to compliance with the principles defined in these Guidelines.

Users shall exclusively use their own private *Hardware* or the *Hardware* made available by GEM on a self-service basis or on loan. They shall not access the *ICS* using other *Hardware*, such as devices available in public areas or belonging to a third party.

Users shall not leave any allocated *ICS Resources* unattended, whether on public transport or in public or private areas.

Users shall take all necessary precautions to prevent or reduce the risks of damage, theft or loss of the *Resources* and the data contained.

If a *Resource made available under a loan* is lost or stolen, *Users* must promptly notify the *ISD* in pursuance of their duty to inform as described in Section 6C in these Guidelines.

All *Resources* made available must be returned to GEM at the end of the *User's* training or at the request of GEM without any need to justify its decision.

B. Storage spaces and data retention

The *ISD* provides *Users* with storage spaces for the duration of his training.

They must save their educational *Documents* on their Workstation or in the *Cloud Drives* provided. Drives are dedicated to specific *Users* or shared between several Users and are configured with access rights that are consistent and compliant with the roles of the different authorized *Users*.

Each *User* may benefit from all or part of the following storage *Resources*, depending on the educational needs defined for their training course, which evolve over time:

- An individual *Cloud Drive*.
- Different shared *Cloud Drives* corresponding to various collaborative workspaces or community exchanges, allowing *Documents* to be shared as part of recurring activities or temporary projects and also in different communities involved in structuring and leading GEM's corporate social network.
- Removable devices, whether belonging to GEM or privately owned, for copying *Documents* onto a mobile storage medium, such as an external hard drive, memory card or writable optical disc.

Cloud Drives include a *Document* version control system that comes in a more or less sophisticated feature. They allow *Documents* to be restored under certain conditions. In case of a personal *Cloud Drive*, *Users* are responsible for restoring *Documents* at their own initiative. For shared *Cloud Drives*, the *Users* sharing the drive will manage independently any restoring of shared *Documents* that may be necessary.

The specific terms for organizing, saving, copying and archiving educational *Documents* are defined jointly by the *User's* School Department, the *teachers concerned* and the *ISD* for the purpose of ensuring data *Security*. *Users* must strictly comply with the different terms and conditions.

The storage of personal or private files on GEM *Resources* is authorized only on individual *Cloud Drives*. *Users* must not store such files on shared *Resources*.

At the end of their training at GEM, and within a period that will be specified in advance, *Users* shall retrieve their personal or private files from any storage space made available by GEM. Otherwise, the data will be destroyed by the *ISD* at the end of the said period and in pursuance of the confidentiality rules specified in Section 6 in these Guidelines.

C. GEM's email system

The *ISD* will provide *Users* with an email account, complete with an email address and personal inbox.

Emails that are received and sent through GEM's email system are checked for viruses and screened for spam. *Users* must immediately notify the *ISD* of any spam filters errors or issues, i.e. if they receive a fraudulent, undesirable or suspicious email, or if they notice that the email system is behaving abnormally.

❖ General principles for using the email system

Any messages are inherently confidential and their dissemination is restricted to the legitimate recipients specified by the sender. As such, senders must check that the recipients can rightfully receive the information that they wish to send. They must not send messages to unauthorized recipients by using the blind carbon copy feature.

All *Users* shall also abide by the following principles for using the email system:

- Use their GEM signature in accordance with the applicable style guide.
- Restrict the number of unsolicited messages sent to their recipients to the strict minimum.
- Check that information is sent to authorized and appropriate recipients.
- If using a distribution list that is available in the collective email directory or created from individual addresses, *Users* must comply with all anti-spam measures. They can also hide certain recipients using the blind carbon copy feature, so that their email address is not disclosed to all recipients. If the list has been created from individual email addresses, *Users* must also indicate how recipients can unsubscribe from the list.
- *Users* can share *Documents* by email as attachments. The type of content and the authorized attachment size must comply with the rules defined by the *ISD* as well as the confidentiality requirements, usage rights and property rights relating to the shared *Documents*. GEM may also restrict the sharing of *Documents* by email and propose alternative methods for collaborative work purposes.
- *Users* shall observe applicable laws and regulations, especially those aimed at protecting intellectual property rights and third-party rights.
- GEM's emails must not contain any content that is unlawful, defamatory, insulting, infringing or likely to constitute an act of unfair competition.

❖ Personal or private use of the email system

Users may use GEM's email system for personal and private communication in accordance with applicable legislation and subject to the principles and rules described in these Guidelines. Personal or private communication must not disrupt the educational or professional use of the email system and generally the operation and performance of the *ICS*.

Users shall not use their GEM email address as an identifier when corresponding on personal or private transactions, especially of a financial or commercial nature, or for authentication on websites allowing for such non-educational transactions. As a non-exhaustive example, *Users* must not disclose or use any GEM email address for personal or private purposes on social networks, forums and blogs that have no educational or professional link to their training at GEM.

D. Use of Internet services

As part of and for the purposes of the attended training, *Users* are provided with an Internet connection for accessing and using *Resources* external to the GEM *ICS*. Use of the Internet is primarily reserved for GEM's educational activities.

Nevertheless, *Users* may use the Internet connection for personal or private reasons, provided that such use is reasonable, in no way disrupts GEM's educational activities and complies with the requirements of applicable legislation and these Guidelines. *Users* shall be particularly vigilant in their private use of interactive multimedia services, which can generate a quantity of network traffic that negatively impacts the performance of the *ICS*. For example, it is particularly important to avoid using VOD streaming services such as YouTube or instant multimedia messaging services such as SnapChat when these services are accessed over GEM's Wi-Fi network.

Users may be granted Internet access to various services offered by GEM as part of their training. They must restrict the use of these *Resources* and the associated data exclusively for educational use unless explicitly authorized by GEM. *Users* shall not reproduce, disseminate or transfer all or part of the said data to a third party, either against payment or free of charge, and irrespective of their relationship with the third party.

This rule concerning exclusive use must be applied to any publication and/or dissemination of information featuring data that *Users* can access as part of their training.

For *Security* and legislative reasons, GEM restricts or prohibits access to certain sites. The process of *Uploadi* and *Download* of files is also checked against criteria based on volume, type of content, property rights and usage rights.

In particular:

- *Users* shall not access certain sites whose content is contrary to public order or decency, i.e. sites offering any sort of justification or support for unlawful acts, sites inciting racial hatred, pornographic sites and generally any site failing to comply with applicable legislation.
- *Users* shall not use the services to propose or provide unauthorized third parties with data and information that are confidential or contrary to applicable legislation or bearing no relation to their training at GEM.

Users shall strictly comply with their duty to exercise loyalty towards GEM. They shall not express any personal opinions that are likely to be detrimental to GEM or its employees.

Users shall not publish or reference any personal or private information on GEM's websites and intranet, except for networks that are specifically designed for that purpose, such as the corporate social network. GEM has reserved certain spaces on its social network to develop communities unconnected with the training course followed by the *Users*, where *Users* can exchange personal or private information in accordance with these Guidelines and the applicable legislation.

❖ Web-based storage and content sharing services

Several storage and content sharing services are available on the Internet:

- Services for sharing *Documents*, contacts and calendars
- Public cloud storage spaces, such as OneDrive or Dropbox
- Digital vaults
- And so on

For *Security* reasons, *Users* must preferably use the equivalent services proposed by GEM and controlled by the *ISD*. If in doubt about the availability or use of an online storage or sharing service proposed by GEM, *Users* must contact the *ISD* to express their needs and submit a service request if necessary.

Public Internet services for storing or sharing information must not be used in such a way that they compromise the *Security* of the said information by undermining:

- Confidentiality: by disclosing information to unauthorized third parties.
- Integrity: by inadvertently or maliciously modifying the shared *Documents*.
- Availability: by inadvertently or maliciously deleting files.

Due to these *Security* risks, *Users* shall not use these web services for storing or sharing educational information or personal information that has been generated, exploited or acquired during their training at GEM.

❖ Social media

Social media have become a key means of communication and are widely used in GEM's digital communication strategy, including the corporate social network, forums, blogs and wikis.

Social media *Users* must behave in a loyal manner towards GEM. Note that each contribution posted on social networking sites brings GEM's reputation into play, and *Users* must respect its brand image and applicable legislation.

6. Protection of ICS Resources by the User

A. Compliance with information confidentiality, integrity and availability obligations

Users must maintain the confidentiality of the information to which they have access:

- The authors have sole power of decision over the distribution and sharing of their *Documents*, in compliance with the confidentiality rules that apply implicitly or explicitly.
- These confidentiality rules may be formally described in *Documents* subject to restricted distribution and/or imposed by technical access control and/or encryption technologies.
- In particular, *Users* must not read any information held by another *User* unless explicitly and legitimately authorized, even if that User has not explicitly protected that information. This rule applies to *Documents* in both electronic and paper format, as well as the following information media:
  - Personal or private written conversations, including emails, faxes and instant messaging, where the *User* is not the direct recipient or has not been copied in.
  - Documents in audio, image and/or video format where the *User* is not a recipient.

Users shall not encrypt the educational data created or accessible in the GEM *ICS*. This requirement may be waived in exceptional circumstances and only in an explicit and formal manner at the *User's* request or if required by the *ISD* due to special confidentiality needs. These needs concern the protection of information deemed to be sufficiently sensitive. Any authorization to encrypt data is explicit, formal and implemented exclusively by the *ISD*. Such permission is granted following a concerted and formalized decision between a GEM authority with sufficient decision-making powers and the *ISD*.

Users must respect the integrity of the information to which they have access:

- In the same way that they agree to ensure the confidentiality of the information to which they have access by strictly complying with the foregoing rules, *Users* shall not modify an information medium for which they do not have express or implied authorization associated with their training at GEM.
- Such modifications concern:
  - The *Document's* contents
  - The metadata allowing *Users* to make advanced use of the Document and enabling the *ISD* to manage the Document
  - The access rights and other technical attributes supporting the *ISD's* requirements for operating and administering the *ICS*.

Users shall comply with the need to ensure information availability:

- By strictly observing the foregoing rules and the provisions relating to the confidentiality and integrity of the information to which they have access, *Users* must ensure that information is sufficiently and exclusively available to the authors and authorized recipients.
- In addition, *Users* shall not move, delete or modify an information medium for which they do not have express authorization from GEM or implied authorization associated with their training at GEM. Specifically, *Users* shall not modify the access rights and other technical attributes supporting the *ISD's* operation and administration of the *ICS*, especially for the purpose of storing, archiving, backing up, restoring and sharing information.

B. Compliance with legislation

In all circumstances, *Users* must comply with:

- Legislation, especially regulations protecting intellectual property rights, including copyright and reproduction rights, and rules of public policy.
- Secrecy of correspondence.
- Confidentiality inherent in the scope of their training at GEM.
- Respect for privacy.

- Protection of *Personal Data*, namely ensuring their confidentiality, integrity and availability by strictly applying the rules described above in Section 6A in these Guidelines.
- Trade secrets.
- Rights to one's image.

C. Duty to inform

Users shall promptly inform the *ISD* of any malfunctions in the *ICS* or any errors encountered when using the *ICS*, including any unusual events or unauthorized acts that may come to their knowledge, such as:

- Smoke or a suspicious odor in or near a *Workstation*.
- Unusual behavior of a *Workstation*, especially when using *Software*, or the appearance of unexpected displays or audio/video signals.
- Loss or theft of an *ICS Resource*, private *Hardware* or *Hardware* provided by GEM, particularly a *Workstation*.
- Intrusion or attempted intrusion in the *ICS* by an unauthorized person.
- Use or attempted use of the *ICS* by an unauthorized person.
- Deliberate or accidental disruption, affecting or potentially affecting the performance of the services provided by the GEM *ICS*.

The notion of providing "prompt" notification is vitally important and necessary to prevent any further adverse effects on the performance of the services provided and to ensure that the *ICS* can be restored to normal operation as quickly as possible. Therefore, *Users* must notify the *ISD* as soon as they become aware of any error, failure or malfunction using what they consider to be the fastest method according to the urgency of the situation, i.e. in person, by telephone or in writing (email).

7. Management of User folders and files

A. During the training period

The folders and files created by *Users* are deemed to be within the scope and for the purposes of the training attended by the *Learner* and therefore part of GEM's *Common Information Assets*. As such, they may be shared with other *Users* in accordance with the applicable confidentiality rules. In addition, they can always be accessed and exploited by the *ISD* for the purpose of ensuring confidentiality, integrity and availability.

Consequently and if necessary, *Users* who have been duly appointed by GEM and assisted by the *ISD*, may access, read, process or transfer all or part of another *User's* individual *Cloud Drive*, without requiring the other *User's* presence. These actions are always carried out under the *ISD's* authority and in strict accordance with the access rights that apply to the folders and *Documents* concerned, depending on the confidentiality level defined by the company.

B. Upon completion of the training

At the end of their training course at GEM, *Users* shall:

- Copy and transfer their messages and *Documents* in accordance with the School Department's instructions. *Users* and the School Department may seek assistance from the *ISD* for accurately defining and carrying out the process for copying and transferring their messages and *Documents*. This retrieval operation mainly concerns the grades and the diploma certificates available in each user’s administrative file on the Intranet.
- Ensure that their emails and their individual *Cloud Drives* do not contain any *Documents* that might be useful to them after their training course, as their emails will be deleted after a certain period following the closure of their *User Account*. They will be informed of the duration of the said period at the end of their training.

The *ICS* access rights assigned to *Users*, including their personal *User Accounts*, are deleted progressively, in line with a calendar transmitted to them in advance, when their training course effectively terminates for any reason. This additional period enables *Users* to retrieve their personal and private *Documents* from the storage spaces made available, as stipulated in the various articles in these Guidelines.

8. Activity control

A. Automated controls

The *ICS* exploits different log files or logs that are automatically generated by the computer and communication equipment. These files are used to maintain the proper performance of the *ICS* and ensure the *Security* of GEM's information by preventing, detecting and manually or automatically fixing failures or faults in the *Hardware* or *Software*.

Consequently, the *ICS* saves and processes a number of internal and external events and activities, including:

- Actual accesses and unsuccessful access attempts to the GEM *ICS* and the information systems belonging to GEM's partners, suppliers and customers.
- Abnormal use and misuse of *ICS Resources*, meaning failure to comply with the rules defined in these Guidelines.

Some log data are retained through computerized *Backups* and *Archiving* and may be used to generate personalized, pseudonymized or anonymized statistics in strict compliance with the provisions of the *GDPR*. These data include:

- The use of GEM's *Business Applications*
- The use of the available system services and *Software*, such as file transfers and sharing
- The use of the *Resources* available on GEM's intranet and the Internet
- Connections to the internal and external networks and the email system, as well as the associated data flows

B. Manual controls

In the event of a fault in any ICS Resource identified by the *ISD* or reported by a *User*, GEM may carry out a manual check of any actions previously performed by one or more *Users* while respecting the confidentiality of the information concerned. These controls are intended to check that:

- The actions performed are suited to the aims of the *Users* carrying out those actions
- The actions causing the reported faults were unlawful, especially when the *Security* of the *ICS* has been compromised.

Under no circumstances shall GEM read any personal or private content, such as defined in Sections 5B and 5C in these Guidelines. In particular, the *ISD*'s involvement will be restricted to checking the technical aspects of the *Cloud Drives* made available for the purpose of maintaining the confidentiality, integrity and availability of any personal or private information they may contain.

However, where controls are required by operation of law or as part of a criminal investigation, GEM may grant access to the folders and files identified as personal or private to any person who has been duly and expressly appointed for that purpose.

If the *ICS* has effectively been compromised or if the risk of a compromise has been identified, the *ISD* will promptly take all necessary measures to restore or maintain the *Security* of the *ICS*. In particular, the ISD may quarantine or destroy malicious *Illegal Files* or files that are considered to be suspicious. The ISD may also temporarily or permanently modify access rights to the *ICS* for a given *User* or *Resource*. These urgent actions may lead to the temporary or permanent loss of availability for the data affected, as well as the loss of their confidentiality and integrity in certain cases. The *ISD* will notify the *Users* concerned or affected by the consequences of the measures taken to maintain or restore the

Security of the *ICS*. The *ISD* will also take a close look at the *User's* reasons and need to use such files or practices that affected the *Security* of the *ICS*. The ISD will propose alternatives that are consistent with GEM's *Security* requirements and the law.

9. Personal data

When carrying out its different missions, GEM is required to collect and process a significant volume of *Personal Data* in its capacity as the *Controller*. This data may concern candidates, *Learners*, graduates, GEM employees and employees from GEM's customers, partners and service providers.

The *Processing* of *Personal Data* is strictly necessary for the purposes of conducting GEM's activities or required by legislation and regulations.

The European *GDPR* and France's Data Protection Act 1978, as amended, set forth the principles for protecting *Personal Data*.

All *Processing* of *Personal Data* must be declared in order to be entered in GEM's *Record of Processing* activities and declared to GEM's *Data Protection Officer*.

Within the context of their training, whenever *Users* have to process *Personal Data*, they must check with their teacher or with the School Department that the *Processing* activity has been declared in GEM's *Record of Personal Data Processing Activities*. If the processing activity has not been declared or if they need help, Users must consult the *Data Protection Officer*.

Users shall:

- Use the *Personal Data* strictly for the purposes for which they were collected or processed.
- Not collect information on beliefs, ideologies, political membership, racial or ethnic origin, sexual orientation or health status.
- Guarantee the *Security* of the *Personal Data* under their responsibility or which they may entrust to *Processors*.
- Comply with the appropriate technical and organizational measures taken to ensure that, by default, only *Personal Data* which are necessary for each specific purpose of the *Processing* are processed.
- Ensure that the data subjects:
  - Are informed of the purposes for processing their *Personal Data* and the retention period.
  - May exercise their right of access, right to rectification, right to erasure, right to restriction of processing and right to data portability with respect to their Personal Data.
- Ask the *Data Protection Officer* for his/her advice or opinion when required to ensure a level of protection for the *Personal Data* in accordance with the General Data Protection Regulation.

Similarly, *Users* are informed that their *Personal Data* are also processed internally by GEM.

The *Transfer* of *Personal Data* outside the European Union is governed by the *GDPR* and France's Data Protection Act 1978, as amended.

10. Retention and Archiving

The retention and *Archiving* of data in the form of electronic files or physical storage media are subject to legal and regulatory obligations, including but not limited to:

- Tax and social regulations
- France's Data Protection Act and the *GDPR*
- France's Act of 1978 on access to administrative documents
- France's Heritage Code requiring administrative documents to be archived

Users shall manage the *ICS* data that they have created, contributed to or received in accordance with legislation and GEM's specific procedures for retaining, archiving and deleting data.

Users shall restrict the recording of *Personal Data* in office productivity *Documents* to the strict minimum necessary, i.e. when the corresponding *Processing* needs are not satisfied by the *ICS Resources* provided. The *Business Applications* use centralized databases for managing *Personal Data* more effectively. Creating or duplicating such data in *Documents* generated by the *User* complicates the process of managing *Personal Data*, especially in terms of changes in sharing, updating and erasure. Such shortcomings in the data management process could lead to the risk of compromised data, which is contrary to the requirements of these Guidelines and the *GDPR*:

- Duplication of discordant information, causing a loss of integrity.
- Access rights maintained without any justification, causing a loss of confidentiality.
- Potential loss of data saved in a storage space without a backup, causing a loss of availability.

11. Liabilities and penalties in the event of a breach of these Guidelines

Any breach of the usage rules and *Security* measures defined in these Guidelines is likely to incur the *User*'s liability and lead to restricted or suspended use of all or part of the *ICS* and even disciplinary measure according to the terms of the study regulation applicable to them, if any.

12. Adoption, dissemination and changes to these Guidelines

A. Effective date

These Guidelines become effective from the moment they are distributed to the *Users* by GEM's Managing Director and the relevant Program Director.

These Guidelines can be consulted from the GEM portal available to *Learners*.

They are brought to the attention of new *Learners* upon enrollment and in the event of revision.

The *ISD* is at the *User's* disposal for furnishing any information about the use of the *ICS*.

Internal communication campaigns are frequently organized to clue *Users* into the best practices when using the *ICS* and its educational, functional and technological environment.

B. Updates

These Guidelines may be updated to reflect:

- Functional, operational and technological changes to the *ICS* that are aimed at maintaining or improving usability, performance and *Security* for *Users*.
- Changes in the risks facing the *ICS*, so that the system can continue supporting GEM's activities with the appropriate level of efficiency and *Security*.
- Legal and regulatory changes.

Any modifications will be subject to the same terms and conditions as the process for adopting these Guidelines.

As stipulated in the foreword, GEM will prioritize the publication of additional best practice guides as a way of formally documenting any of the above updates when they are likely to lead to a change in the functional rules for using the *ICS* or maintaining *Security*.

Exhibit: Glossary

The following terms used in these Guidelines will have the meanings set forth below:

Archiving: computer operation for retaining and filing *Documents* or generally files that are no longer actively used and which do not have any immediate value for a given GEM activity. This process involves computer data that have become static as opposed to dynamic data, which continue to change and/or which are still exploited by GEM *Users* as part of their educational activities. The retention period varies according to the type of data. Data are subject to minimum and maximum retention periods. The period may be imposed by legal, regulatory or contractual requirements or defined by GEM for the purpose of satisfying its functional needs, but without affecting the performance or operating / management costs of the *ICS*. By extension, archiving is carried out by the *ISD* as a clearly identified service that is tailored to the educational needs of the relevant *User*.

Backup: service for protecting identified information contained in the *ICS* by copying the information onto a physical storage medium that is different to the original storage medium. This service should be distinguished from the *Archiving* service.

Business Application: IT application for managing a specific GEM activity by computerizing and automating certain management processes. Business Applications are not only specific to a business function but also to GEM, for which it must represent the business processes, which are different to the processes used by another structure performing the same business activities but in a different way.

Cloud Drive: storage space made available by an outsourced storage service, which can generally be accessed over the Internet. The physical storage devices providing the *Cloud Drive* are not hosted in the infrastructure of the physical *ICS Resources* belonging to GEM but in an external and remotely accessible third-party infrastructure.

Common Information Assets: also known as information capital, these assets contain all the proprietary knowledge, expertise and other information possessed by an organization, which its members can use and implement to perform their own activities. These assets are GEM's property. They are protected by and subject to copyright and intellectual property rules.

Controller: means any entity that determines the purposes and means of the *Processing* that it implements itself or that it has charged a *Processor* to implement.

Data Protection Officer: a natural person mandated by a given structure to inform, advise and ensure that employees are aware of the level of protection for *Personal Data* in accordance with the General Data Protection Regulation. The data protection officer reports directly to the highest management level of the *Controller* or the *Processor*.

Document: an intelligible file used to provide information or proof in text, image, audio or video format. These Guidelines make a distinction between *Documents* and other computer files, which do not provide information or proof for GEM's functional requirements or for *Users*, but which are created, recorded or processed by certain *ICS Resources* for the system's intrinsic operation.

Download: the act of fetching one or more computer files from a server or remote computer over a public or private corporate communication network. The opposite of *Download* is *Upload*, which involves sending such files to a server or remote computer via a similar connection.

GDPR: the General Data Protection Regulation is the European regulation that defines the new unified legal framework throughout the European Union for protecting *Personal Data*. It strengthens the rights of data subjects and gives added responsibilities to entities processing their data. The Regulation's reference is EU 2016/679.

Hardware: all or part of a computer or communication device, including a spare part of such a device. The *Hardware* goes hand-in-hand with the *Software*, which may be standalone or a fully incorporated and inseparable part of the Hardware. A Hardware device contains internal components that are essential for its operation, while other components are secondary or optional. Certain additional parts or other standalone devices may be added to the outside of a device and therefore constitute peripherals that extend the device's functional or technical capacities. Internal or external parts are used to receive, send, store and process information. All operations are performed in accordance with the instructions contained in the *Software* and in compliance with the handling of the peripherals acting as an interface between a *User* and the *Hardware*, known as a human-machine interface. Unless otherwise stipulated, the term is used in these Guidelines to describe any hardware *Resource* of the *ICS* that delivers or helps to deliver services supporting the *User's* activity, whether educational, functional or informational.

ICS: GEM's Information and Communication System is designed to satisfy and support the company's business requirements by providing two types of core *Resources*: *Business Applications* and *Workstations*. To ensure that *Users* can access and use these tangible components, the *ICS* is built on a complex infrastructure of hardware and software *Resources* and specialized services, including servers, computer and telephone networks, *Security* and storage management devices, and directory and email services.

ISD: Information Systems Division. The *ISD* is one of the operational divisions reporting to GEM's Secretary-General. The division is responsible for aligning the *ICS* with business needs and ensuring the system's performance and *Security*. The *ISD* enforces the rules specified in these Guidelines.

ISD Personnel: all the members of GEM's *ISD* performing the following activities:

- Design, management, upgrades and corrective maintenance of the *ICS*.
- *User* support and assistance.
- Security of the data in the *ICS* and measures to ensure *Security*.

Illegal File: this term includes files with illegal content and/or files that have been accessed or acquired in an illegal manner, i.e. against the law. For illustration purposes, this includes but is not limited to content or access / acquisition methods that are contrary to public order and decency. In particular and in pursuance of these Guidelines, they must fulfill the integrity requirements of the information contained and comply with copyright and intellectual property rights.

Learner: person enrolled on a GEM training course.

Personal Data: any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an digital identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processor: means a natural or legal person, public authority, agency or other body which processes *Personal Data* on behalf of the *Controller*. *Processing* by a *Processor* is governed by a contract or other legal act under Union or Member State law, that is binding on the *Processor* with regard to the *Controller*.

Processing: means any operation or set of operations which is performed on *Personal data* or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Record of personal data processing activities: a register that contains all the *Personal Data Processing* activities. The record contains the following information: the purposes of the *Processing*, the categories of data subjects, the categories of personal data, the categories of recipients, the storage periods, a description of the technical and organizational *Security* measures, and transfers of personal data to a third country or an international organization.

Resource (of the *ICS*): in addition to the actual *Workstation*, a resource represents any IT service or application that the *ISD* makes available to *Users*. In addition to all of GEM's *Business Applications*, a few examples of *Resources* are as follows:

- Standard applications: emails, office productivity software and web applications
- Peripherals: printers, *Document* scanners, external hard drives and access badges
- External services: these services act as a functional extension to the *ICS* by offering a new service or outsourcing an existing service. Examples as of Thursday, June 20, 2019: Microsoft Exchange Online enterprise messaging, Secure Print remote printing, encoding and updating of secure access badges, and access to specialized online documentary *resources*.

Security: this term corresponds to different expressions, including "information systems security", "IT security" and "cybersecurity". In these Guidelines, *Security* concerns the *ICS* as a whole, but especially data in the form of *Documents*. Security encompasses all the technical, organizational, legal and human means necessary for implementing measures to prevent unauthorized use or modifications, and unintentional and deliberate misuse of the *ICS*. The *ISD* defines and ensures the *Security* of the *ICS*, whose long-term purpose is to continue inspiring trust in *Users* and customers. The medium-term purpose is the consistency and performance expected from the entire *ICS*. The short-term objective is for each *User* to have access to the information that they legitimately and legally need and in accordance with these Guidelines. The three characteristics that define the required level of *Security* for an *ICS Resource* are availability, integrity and confidentiality. Once the security objectives have been determined, the risks facing each *Resource* can be assessed according to the Resource's intrinsic vulnerabilities and threats to which the Resource is exposed. The *ISD* defines and implements the necessary precautions and countermeasures to achieve the specified *Security* objectives. The ISD has mandated the Chief Information Security Officer to help to define the objectives and to contribute towards their achievement.

Software: a collection of instruction sequences that can be interpreted by a machine and a set of data required for such operations. Therefore, the *Software* determines the tasks that can be performed by the machine, schedules its operation and gives the machine its functional utility. The sequences of instructions (known as a program) and the data in the *Software* are usually structured into files. Implementation of the instructions in the *Software* is known as execution, and the machine is called a computer or a calculator. *Software* may be described as system or application software, as standard or bespoke, and finally as proprietary or free, depending on several criteria including the way in which the Software interacts with the *Hardware*, the vendor's business strategy and the rights to the program source code. Unless otherwise stipulated, the term is used in these Guidelines to describe any software *Resource* of the *ICS* that delivers or helps to deliver services supporting the *User's* activity, whether educational, functional or informational.

Transfer of personal data: means any *Processing*, any communication, any access, copying or moving of *Personal Data* for processing in a country outside the European Union.

Upload: the act of moving one or more computer files to a server or remote computer over a public or private corporate communication network. The opposite of Upload is *Download*, which involves fetching such files from a server or remote computer via a similar connection.

User: any Grenoble Ecole de Management *Learner* who access or use the *ICS Resources* at GEM's sites or remotely, and to whom these Guidelines apply. The types of Users concerned are specified in Section 2A in these Guidelines.

User Account: practically speaking, a *User Account* identifies and authenticates *Users* in the GEM *ICS* from an authorized *Workstation*, so that they can use all the Resources allocated to their account. User accounts are associated with a unique username and a password meeting predefined security requirements. To be more precise, a *User Account* is a specific *Resource* in the *ICS* containing the rights that have been assigned to a *User*, a group of *Users*, the *Resource* itself or a group of *Resources* for accessing and using the *ICS*. If assigned to one or more *Users*, the *User Account* may be individual and reserved exclusively for a given *User* or it may be collective and shared between several *Users* who have been duly authorized to use the account. In addition to the assigned access and usage rights, other data may be used to define a *User Account*. For a given *User* of the *ICS*, such additional data relate to their identity, their place within GEM's organization, their geographic location, their contact details and so on.

Workstation: from a computing viewpoint, it mainly represents the access point to all the functionality of a *Resource* in the GEM *ICS*. Whether a computer, tablet, smartphone or simple handheld terminal, the *Workstation* provides access to and use of the IT applications and services that GEM makes available to *ICS Users* according to the needs of their educational activities. By extension, the *Workstation* includes all the peripheral devices, software and hardware, whether individual or shared, that are necessary for using the applications and services. It also includes all the documentation required to manage and correctly use the ICS.

The following online reference sources have been used for certain definitions: Wikipedia and Larousse.