GUIDE

FOR USERS OF THE VINCI GROUP'S INFORMATION SYSTEMS

JUNE 2018

CONTENTS

Only the French version of this document is binding on the VINCI Group.

FOREWORD

Today, information systems are crucial to ensuring satisfactory operation and performance of companies. Since substantial competitive, financial, legal and image risks may arise from malicious acts, failure to take precautions or improper use of resources, raising users' awareness and informing them of their responsibilities is vital, as is strengthening means of protection and control.

In this context, this Guide defines:

- the general rules governing use of IT system resources;
- prohibitions and particular precautions to be taken concerning all kinds of data, all kinds of data processing, all components of IT systems, all communication tools and all equipment made available by the company;
- the principles of protection and control that may be put in place.

The Guide therefore specifies the rights, duties and obligations of the user concerning use of information system resources.

Fields of application of the Guide

The Guide is addressed to any user of the company's information system resources.

A "user" is any person, whatever their status (notably employee, temporary staff, trainee, consultant, service provider), who is tasked with using these resources.

By "resources" we mean:

- Equipment for all types of IT systems (notably computers, software, printing peripherals, internal networks, shared servers, detachable storage devices);
- all means of communication;
- information and data (notably files and databases).

All these resources made available to employees, together with their content, remain the property of the company.

The Guide applies to all countries in which the Group conducts operations. If required, it may be complemented with add-ons that take into account the specific needs of countries and entities.

General rules governing use of the resources

Access to resources

Authorisations to access the resources are issued by the company to each user on an individual basis and in line with their duties and assignments.

These authorisations are strictly personal and may not, as a matter of principle and under any circumstances, be transferred, loaned or transmitted, in any way whatsoever, to a third party inside or outside the company, even temporarily.

Any modification of the user's professional status may give rise to a modification of the authorisation.

Any new authorisation requires the user to make a prior specific request in accordance with the procedures in force.

Authorisations may be suspended, modified or withdrawn, in accordance with access authorisation and management procedures, in particular in the event of a recognised risk to the effective operation of IT systems.

All authorisations expire when the individual suspends or puts an end to their professional activity, and at the latest at the time the employment contract is terminated.

Principle of use of the resources

The resources are made available to users, for the purposes of professional use, in the framework of their attributions in relation with the tasks entrusted to them by virtue of their employment contract.

All these resources, together with their content, remain the property of the company.

The user is, however, responsible for them and contributes to their security, at his/her particular level.

Use of the resources must not bring the company's legal liability into play or harm its image. In particular, these resources may not under any circumstances:

- be used to carry out personal activities of a commercial nature;
- disrupt or restrict professional use of the company's resources, their maintenance or their security (which includes their confidentiality, availability and integrity).

The user must not under any circumstances engage in any activity contrary to the law or which might harm the company's image or the security, integrity or performance of its information system.

Right to disconnect

The terms of the right to disconnect mentioned below aim to raise users' awareness and empower them.

Accordingly, users are invited* to:

- avoid sending emails and SMS messages and making calls outside regular working hours;
- where appropriate and if the email client so permits, use the deferred email sending function;
- specify a deadline for reply in their message;
- indicate that they are unavailable via an absence message and if possible transfer to an available contact person;
- deactivate notification of emails outside of regular working hours.

Users are also reminded that it is not compulsory to answer emails, SMS messages or calls outside of regular working hours*.

Finally, the importance of exemplarity of the management line regarding the reasonable and rational use of digital tools should be stressed.

Use of Internet services

Internet access is granted individually to users and made available for professional use. It is configured and administered for this purpose.

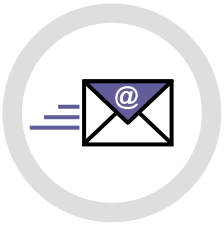
So as to avoid compromising the general level of security, users must use Internet services in compliance with all legal regulations and rules governing the websites visited.

They must not:

- connect or attempt to connect other than via the official Internet access provided through the company network;
- visit websites likely to incur a risk for the security of the resources, or to compromise the confidentiality of information;
- more generally, use Internet services for commercial, leisure or illicit purposes.

* Except in special cases, e.g. on-call duty.

Furthermore, users are reminded that in the context of executing their professional contract, all employees must comply with an obligation of loyalty. This obligation also applies to public Internet spaces and more particularly to blogs, forums and social networks. Any disclosure on this type of site, on any social media or on the Internet in general of information belonging to the company or harms its image is strictly forbidden.



Use of electronic messaging systems

Access to the company's electronic messaging systems is made available to users for professional purposes.

To meet resource availability and performance requirements, messages must remain limited in volume and number. The IT Department reserves the right to limit the maximum size of messages, mail-boxes and certain types of attached files.

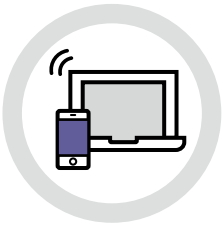
When sending messages, users must pay particular attention to the appropriateness of the list of recipients and the presentation, content and size of the message.

They must take care to obey the following rules:

- explicitly indicate the subject of the message;
- use internal and external dissemination lists with precaution;
- remain especially vigilant regarding all communication of personal data (see paragraph Concerning personal data protection, page 10);
- do not pass on internally messages that potentially contain viruses (if in doubt contact the IT Department);
- do not transmit outside the company network messages or attachments containing confidential content (if necessary, contact the IT Department) or likely to harm the reputation of the company;
- never disseminate address books or organisation charts outside the company.

Concerning reception of messages:

- any suspicious, non-legitimate, unsolicited message (sender and domain name unknown, messages without a subject, or whose subject is overtly commercial or alluring, etc.) must be deleted without being opened and without clicking on any related links or opening attachments;
- users must take care to be particularly cautious as regards subscription to public distribution lists, which often serve as sources for unsolicited advertising messages (Spam) and spreading of viruses through impersonation.



Mobility

Users of laptop computers and all types of mobile terminals undertake to scrupulously secure and protect their equipment and access to the data it contains, whether in their own country or abroad and, in particular, in individual or public transport.

In the event of disappearance of an IT device, following loss or supposed or proven theft, users must, imperatively, alert the IT Department by any means at their disposal and as soon as possible, so that the measures required to protect the company's IT system can be put in place.

In parallel, they must make a report of the event to their manager to enable an assessment to be made as to the potential damage for the company.

When connecting to the company network from a public place or a work station not belonging to the company, users must take care not to enter their connection password from the Internet browser and to close down any open sessions, delete any browsing history and any software used to establish the connection.

Users must also take care not to store information of a professional nature on any hardware other than that made available by the company.

Lastly, all users must connect their laptop computer to the company network as regularly as possible to ensure that maintenance operations and operations to upgrade protection procedures are carried out in accordance with the company's security policy or with best practices in this field.

Conformity of hardware, programs and applications

Hardware

To guarantee the best possible match between individual hardware (computers, work stations, etc.), IT system applications and the network, the company provides standard configurations. For this reason, the IT Department must validate any installation of hardware not provided by it, even if it is hardware strictly identical to that already in service.

Detachable storage devices (USB keys or external hard disks) can be conduits for the entry of viruses into work stations and the network. They must be used with caution, particularly when they come from outside the company.

If in doubt, users must contact the IT Department, which will carry out the appropriate security controls. Furthermore, given their small size which makes them vulnerable to theft, it is essential to delete files from them once the data transfer has ended.

Lastly, in the event that there is no pre-defined configuration for a specific need, users must contact the IT Department to examine the best solution for responding to the need expressed.

Loaning and selling hardware

It is forbidden to loan, sell or assign to third parties the equipment provided by the company.

Software and applications

Software configurations are defined by the company to respond to user needs. Any attempt to modify the initial configuration is forbidden since it is likely to cause major dysfunctions in the resources (compromising performance, safety, etc.).

In the event that there is no pre-defined configuration for a specific need, the user must contact the IT Department to examine the best solution for responding to the need expressed.

Lastly, with the aim of guaranteeing a constant level of security and performance, it is forbidden to block automatic software-update procedures.

Individual IT developments

IT extensions developed using office automation tools (macros, databases, etc.) and their maintenance are placed under the full responsibility of the users who developed them.

Loan and sale of software or licences

In accordance with the legislation governing intellectual property, the company pays software royalty and licence fees.

Consequently, it is forbidden to loan, sell or assign to third parties software, licences, installation programs and tools provided by the company. This prohibition also covers software developed by the company's internal IT teams.

Security and data protection

Each user contributes to the security and protection of the resources, in particular of the data processed, and undertakes to avoid deliberately by-passing, disrupting, disturbing, interrupting or eliminating security (antivirus, etc.), filtering or control procedures put in place by the company.

Users are required to alert the IS department as soon as possible whenever they notice any malfunctions or anomalies (including but not limited to instances of information-system hacking). They are also required to alert their line manager if they realise they are able to access any resources above their security clearance level.

Concerning electronic messaging and the Internet

Electronic messaging is not a secure communication channel in respect of messages sent to outside the company.

While the company has the capacity to control its internal network, it has, conversely, no visibility or means of action once data is circulating on the public Internet network. It is therefore advisable to assess the sensitivity of information before transmitting it to third parties outside the company using this communication channel.

Furthermore, the mechanisms for protecting office-automation files by means of passwords freely proposed in publishing applications (Word, Excel, PowerPoint, PDF, etc.) do not provide effective protection, in the sense that they can be easily by-passed using software freely available on the Internet.

Therefore, if professional imperatives require users to exchange particularly sensitive data with a third party outside the company, they must contact the IT Department for their entity to obtain a solution meeting the requisite confidentiality needs and compatible with the company's resources. Where the company is legally required to set up a system to log* and filter** Internet connections, messaging systems and data exchanges, it must make all necessary declarations with the relevant supervisory bodies.

* The log contains technical information about the connection such as the time it occurred and the user's IP address.

** Filtering connections to Internet sites may involve unencrypting the data exchanged by the user's workstation and the website. This analysis is carried out in aggregate: the unencrypted data is not recorded (information is inaccessible). The configuration for systems that log unencrypted flows is the same as the one for ones logging standard HTTP flows (time, user account, website URL, access authorisation, virus identified). No other information is recorded.

Concerning use of cryptographic means

Users must use only solutions approved by the company to protect data.

Concerning protection of the work station

Authorisations to access resources, including the work station, are issued personally to each individual user. In this context, in order to protect access by a third party, whoever it may be and even on a one-off basis, each user must:

- apply the company policy relating to passwords (renewal, sufficient length, complexity, etc.) to gain access to the resources;
- never divulge their passwords, which must in no case be transferred, loaned or transmitted in any way whatsoever to a third party inside or outside the company, even temporarily (subject to urgent service requirements, in which case the password will need to be changed);
- lock their work stations when they are absent and turn them off at the end of the day and on the weekend, except for technical imperatives involving maintenance of the resources or operational requirements;
- not exploit and/or divulge any security flaw brought to their attention that might affect the resources made available to them and must inform the IT Department as soon as possible;
- not seek to by-pass or deactivate the protective systems installed on work stations (antivirus, firewall, etc.);
- use the means made available to them by the company to secure work stations;
- carry out back-ups of their work station. In the event of dysfunction, they must inform the IT Department.

Remote intervention in a user session can only take place after a prior request for assistance by the user, or at the prior request of the IT Department, with the authorisation of the managers concerned. Only people approved by the company are authorised to carry out any operations on the resources made available to users.

Concerning business continuity

For reasons of business continuity, users must, in the event of absence, put in place the necessary delegations of authority enabling access to their professional data and must not communicate their personal access codes to third parties.

Users must, in addition, regularly back up and archive the data they use, create or process for the purpose of service continuity by using the software, hardware and/or procedures made available by the company, and notably network spaces.

On cessation of his/her activity, the user must hand over to the company, in addition to all hardware with which he/she was entrusted, the dossiers, directories, files, e-mails and, more generally, any electronic document of a professional nature to enable business continuity.

Concerning personal data protection

When carrying out their duties, users may be required to access personal data (of employees, prospective clients, clients or partners for example) and they must recognise the confidential nature of such data.

The term "personal data" covers any information regarding a natural person that is identified or identifiable. An "identifiable natural person" refers to a natural personal that could be identified either directly or indirectly, in particular through the use of ID details, such as a name, ID number, location data, online ID, or one or several specific elements relating to a person's physical, physiological, genetic, psychological, financial, cultural or social identity.

Therefore, users must take all necessary precautions in the framework of their attributions in order to protect the confidentiality of the data to which they have access, and in particular to avoid them from being communicated with persons that are not expressly authorised to receive such data.

Therefore, users are requested to:

- avoid using, copying or analysing personal data that can be accessed for reasons other than those intended by their attributions;
- disclose data only to those duly authorised, by virtue of their position, to receive such data, whether it concern private or public individuals, natural or legal persons, and in situations expressly set out in the company's policies;
- avoid copying such data except when strictly necessary;
- take all necessary precautions in the framework of their attributions to avoid fraudulent or unauthorised use of such data;
- inform their line manager as soon as possible of any communication to third parties, loss, destruction or accidental alteration of personal data;
- take all precautions, in particular concerning security, to protect the physical and logical security of such data (for example, the requirement to input a username/password and keep the resource connection password confidential).

Control of use of the resources

In compliance with the principles of transparency and proportionality, for security purposes and to verify correct access to the company's resources, satisfactory operation of the information system and to ensure that it does not incur civil or criminal liability in respect of use of the resources by users, the company reserves the right to carry out regular verifications and controls.

For this reason, the company implements and ensures correct operation of filtering and control procedures (notably firewall, access control systems and traceability systems) concerning use of the company's resources (notably the Internet, electronic messaging, shared network services, fixed and mobile telephony).

These systems may be implemented, notably as concerns electronic messaging, to control any incoming or outgoing message (anti-virus control, anti-spam control, control of integrity, size, list of recipients, etc.) and also to block, notably on the basis of a list of keywords, messages, electronic exchanges or access to unauthorised websites.

Implementation

Dissemination

Each entity of the company is responsible for disseminating this document.

Compliance with the laws in force

In the context of use of the resources made available to them, users undertake to comply with this Guide, and also to comply with the laws and regulations in force in their country.

Sanctions

Failure to comply with the rules and measures described in this Guide may bring the user's personal liability into play or, in the case of a service provider, that of the company employing him/ her. If it can be proved that the user is personally responsibility for such failure, he/she may incur disciplinary penalties as provided for in the internal rules and regulations or legal proceedings in compliance with the applicable law.

R E A L
SUCCESS
I S T H E
SUCCESS
YOU SHARE

June 2018 edition – GSI-2018-06-EN – Photo credits: rawpixel.com from Pexels – Design: www.gcommeuneidee.com

VINCI
1, cours Ferdinand-de-Lesseps
92851 Rueil-Malmaison Cedex
Tél. : + 33 1 47 16 35 00
www.vinci.com