VINCI GENERAL POLICY

CYBERSECURITY

JUNE 2019

EDITORIAL

As threats against our information systems are becoming increasingly sophisticated and frequent, fighting cybercrime has become a priority for our Group.

Protecting VINCI's assets and information is a strategic issue for reasons relating to competitiveness, trust and data protection. With digital technologies gaining ground in all our business lines, our Group has taken measures to reinforce the mechanisms it uses to protect its data, secure its information systems and maintain its operational performance.

Although financial services are particularly exposed to cyber risks, due to the potentially serious repercussions of attacks on our secure payment systems, all of the Group's business lines, transformed by the digital revolution, are now concerned. This is why every employee needs to be aware of cyberrisks and pay attention when he or she notices anything unusual. But cybersecurity also requires a comprehensive approach including all the stakeholders in our ecosystem (suppliers, service providers, partners, etc.).

This document describes the Group's general cybersecurity policy. It specifies VINCI's policy framework relating to cybersecurity for all the Group's information systems and presents the roles and responsibilities of everyone involved.

I am counting on your commitment to applying and enforcing these security rules so that we can collectively safeguard VINCI's operational performance in the best manner possible.

Christian Labeyrie

VINCI Executive Vice-President and Chief Financial Officer, VINCI

FOREWORD

In order to defend against an evolving panoply of cyber threats, it is essential that we significantly strengthen the security of our information systems.

Following an overview of the issues and risks relating to cybersecurity, this document aims to:

- set out the key principles and rules to ensure the protection of our data and our information systems.
- define how cybersecurity capabilities are organised within the Group, as well as the roles and responsibilities of all parties involved.

It applies to all VINCI business lines, divisions and entities worldwide. Everyone is duty bound to apply this policy, taking account of their local contexts and specifics, particularly in light of their cultural, legislative and regulatory requirements.

VINCI's general cybersecurity policy is proposed by the Group's Chief Information Security Officers (CISOs), validated by the Cybersecurity Strategy Committee and approved by VINCI's Executive Committee.

All of VINCI's business lines and entities are collectively responsible for the implementation of measures to protect our assets and our data. The Group's employees are also required, at their level, to adopt responsible digital behaviors to address threats and vulnerabilities.

This document will be updated as and whenever necessary in response to changing threats.

NEW INFORMATION SYSTEMS AND THE ATTENDANT RISKS

The digital transformation of VINCI's business lines promises numerous development opportunities. But it also presents new risks and threats – with the proliferation of communication channels, the Group's exposure to cyber risks has increased – and greater pressure is being brought to bear by regulators.

Five technology trends have an impact on our information systems and our everyday life

1 Cloud computing

While the cloud offers universal access to IT services and applications, it entails the delegation of security responsibility to service providers. This in turn imposes new responsibilities on internal security teams (in particular relating to governance, compliance and audit).

2 Greater mobility

The ability to access information systems from any network and workstation has generated new practices such as remote and working (whether from home, another site or as a digital nomad), as well as greater freedom in the organisation of work. This mobility increases the exposure of the information system.

3 Big data

Big data technologies improve the processing time for high volumes of complex data. Given the expanding array of data sources, the challenge is in the classification of data (private, public, etc.), so as to apply the appropriate security measures. Big data also allows the movement and consumption of the data to be analysed, thereby enabling us to better anticipate certain security incidents.

4 Internet of things (IoT)

IoT enables data interchange between non-traditional computer systems in real time and opens up very promising possibilities for the future. IoT assumes constant network availability and poses crucial questions with regard to data security.

5 Artificial intelligence (AI)

New artificial intelligence (AI) technologies are destined to further accelerate and automate the processing of information. In this respect, AI plays a part in spreading malware, but it can also help protect information systems by improving the capacity to respond to security incidents.

Major risks

The cybersecurity process strives to mitigate the consequences of the following four major risks:

MAJOR RISKS

CYBERATTACKS

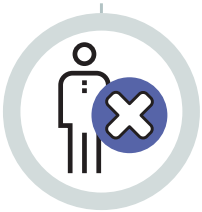
Malicious acts against a set of IT resources.

INFORMATION LEAKAGE

Loss or disclosure (untimely or intentional) of data.

CYBERESPIONAGE

Eavesdropping or theft of confidential and/or competitive data for financial gain.



FRAUD

Intentional act by a third party or employee aimed at misappropriating Group assets.

CONSEQUENCES

DAMAGE TO REPUTATION

The potential impact of an incident on the Group's image or that of any of its brands.

FINANCIAL LOSS

The potential impact of an incident on the Group's earnings or share price.

DENIAL OF SERVICE

The inability of an information system component to provide services.

NON-COMPLIANCE

Judicial, administrative or disciplinary sanctions as a result of a failure to comply with legal or regulatory requirements or professional standards.

Failure to meet obligations (legal, regulatory, professional, contractual) resulting from data leakage or a flaw in the information system, is also a risk in itself.

Any malfunction in information systems can have far-reaching consequences for the Group's activities, such as interruptions of certain services rendered, financial losses, administrative sanctions, civil or criminal penalties or reputational damage.

Cybersecurity controls should be designed to pre-empt threats, minimise risks to our information systems and mitigate their impact.

The levels of security and protection are proportional to the issues at stake for each business line and adapted to each information system; they also evolve to respond to the changing threat landscape.

VINCI'S APPROACH TO CYBERSECURITY: 10 KEY PRINCIPLES

VINCI's approach to cybersecurity is underpinned by the 10 principles presented below. Each principle comes with a set of rules, which apply to all Group entities.

01.

VINCI's Executive Committee is the sponsor of the cybersecurity process

The Executive Committee validates the action plans proposed by the Group's Chief Information Officer (CIO) after examining the security levels in place, and according to the acceptable level of risks for our activities. VINCI's Chief Information Security Officer (CISO) is responsible for supervising cybersecurity action plans. VINCI's CIO reports to the Executive Committee on progress against these plans.

- The Executive Committee allocates a budget for cybersecurity.
- The Chief Information Officer regularly reports to the Executive Committee on evolving threats and on progress against action plans.

02.

Cybersecurity actions are coordinated by a Group-wide community

A community comprising the CISOs of all VINCI's business lines, divisions and entities takes actions relating to cybersecurity. This community is supervised and coordinated by VINCI's CISO.

- Communications between CISOs must remain confidential within this community.
- CISOs across the Group are required to report every security incident to VINCI's CISO. The other CISOs are also informed of any such incidents.
- The CISOs work towards the best interests of the Group at all times and are expected to share any lessons learned. Their actions must be communicated to VINCI's CISO, thereby contributing to the advancement of the Group's overall maturity in this respect.

03.

The subsidiarity principle applies

Mandatory security measures are determined for the Group as a whole. Each business line and entity is duty bound to implement them and can then establish additional measures at its own level. In accordance with Group organisation and its cybersecurity strategy, all VINCI entities are responsible for implementing security measures.

- The CISOs take part in defining the Group's mandatory security rules.
- They ensure that these rules are followed in their entity and are accountable to VINCI's CISO in this respect.

04.

Each entity must be prepared for a cybersecurity crisis

The CISOs must map the specific threats they face and establish crisis management procedures so that each entity is able to react correctly in the event of an incident.

- Each entity determines the persons to contact in the event of a security incident.
- They must define their own crisis management procedure and test it at least once a year.

05.

Cybersecurity policy is proportionate to the level of risk

Security measures are designed to consider all types of risk and are then adapted to each asset. Each entity must ensure that the "security by default" principle is applied for all new services. Exhaustive coverage of risk is not a reasonable objective: it is important to concentrate on the essentials, and through mitigations supported with arguments, to accept residual risks that have been properly assessed with full knowledge of the facts.

- The CISOs must confirm that the major risks defined by VINCI are consistent with their local specifics.
- Each entity must list their critical systems and keep this inventory up to date.

06.

Users are the first line of defence

It is up to each user to behave responsibly and appropriately to guard against risks.

- The CISO community has a duty to raise users' awareness of security questions. It must also present and explain the procedures, tools and best practices to them.
- Employees must read and understand the VINCI Group Guide for Users of Information Systems and attend cybersecurity awareness-raising sessions. They undertake to abide by information system user best practices as recommended by the community of CISOs.

07.

Security measures designed to be as non-invasive as possible for users

Security measures must, as far as possible, be simple and comprehensible by everyone. They must always factor in the needs inherent to each business line and not significantly disrupt the user experience.

08.

Improved levels of security are guaranteed by regular controls

As with any activity, the process of improving cybersecurity also consists in defining and implementing controls and in reporting on their results.

- The design of the systems must not just factor in such controls but also facilitate them.

09.

Cybersecurity complies with the law and regulations

Each business line is responsible for ensuring that their action plan factors in and complies with the law and current regulations.

10.

The cybersecurity process is reviewed on a regular basis

Cybersecurity forms part of a continual improvement process. Within this framework, it must be monitored and the associated process must be reassessed at regular intervals.

GOVERNANCE OF VINCI'S CYBERSECURITY

Parties involved and their responsibilities

VINCI's Executive Committee

The Executive Committee validates VINCI's cybersecurity policy and strategy. It oversees the rollout of the cybersecurity policy and the related controls.

VINCI's Chief Information Officer

VINCI's Chief Information Officer keeps the Executive Committee regularly informed of changing threats and of progress against the action plan. He/she chairs VINCI's Cybersecurity Strategy Committee.

Chief Information Officers in the business lines

Chief Information Officers accross the Group implement cybersecurity measures and allocate the necessary budgets. They ensure that the cybersecurity strategy is integrated into their business line's overall information systems strategy.

VINCI's Chief Information Security Officer (CISO)

VINCI's CISO draws up the cybersecurity strategy together with the CISOs of the business lines, and submits it to VINCI's Chief Information Officer.

He/she coordinates VINCI's action plan and ensures it is implemented in the business lines. He/she communicates the level of cybersecurity risk. He/she coordinates the network of CISOs in the business lines and disseminates Group rules and best practices.

CISOs in the business lines

The CISO in each business line is responsible for adapting and applying VINCI's cybersecurity policy within his/her area of responsibility. He/she must factor in the local threats and specifics in order to put in place a cybersecurity policy tailored to the needs of the business line.

He/she participates in VINCI's cybersecurity transformation programme and is required to monitor the local action plan. He/she reports cybersecurity incidents and key indicators to VINCI's CISO.

Other parties involved

Cybersecurity is a key concern for VINCI. The Group is organised with a view to collaboration and participation in the measures required to achieve cybersecurity objectives:

- The Audit Department monitors cybersecurity measures.
- The Data Protection Officer (DPO) defines measures concerning privacy.
- The Legal Department and IT Purchasing Department define cybersecurity clauses in contracts.
- The Security Department guarantees the physical security of people and assets.
- The Human Resources Department rolls out awareness and training programmes to all users.
- The Communication Department plays a key role in to cybersecurity-related crisis communication.
- The project managers assess the business impacts of cybersecurity.
- External authorities (ANSSI, CNIL) provide assistance and support in the event of a cybersecurity incident.

VINCI's cybersecurity bodies and their roles

VINCI's Cybersecurity Strategy Committee

VINCI's Cybersecurity Strategy Committee, chaired by VINCI's Chief Information Officer and coordinated by VINCI's CISO, meets every six months. Its role consists in:

- validating VINCI's cybersecurity strategy and allocating the resources and budgets needed to implement it;
- receiving and analysing information on itself with cybersecurity incidents within the Group and managing major crises;
- examining key cybersecurity performance indicators.

Members: VINCI's Chief Information Officer, the Executive Committee's IS expert, VINCI's CISO, VINCI's Chief Audit Officer, VINCI's Security Officer.

VINCI's Cybersecurity Steering Committee

VINCI's Cybersecurity Steering Committee, which is chaired by VINCI's CISO, meets every month.

Its responsibilities include:

- drawing up VINCI's overall cybersecurity strategy and submitting it for validation;
- steering VINCI's cybersecurity transformation programme and implementing projects in the business lines;
- producing key cybersecurity performance indicators.

Members: VINCI's CISO, the business lines CISOs.

Cybersecurity Pivot Club

The Cybersecurity Pivot Club, which is coordinated by VINCI's CISOs, meets every three months. Its main objectives are to:

- provide information about VINCI's cybersecurity transformation programme and collect feedback from the field;
- qualify and formally record feedback and communicate about industry best practices and those applied within the Group;
- carry out technological and regulatory monitoring.

Members: VINCI's CISO, the business line CISOs, security experts, cybersecurity and IT security experts, network and systems managers, and business line staff, depending on the agenda.

Role of the Information Systems Steering Committee

The Information Systems Steering Committee, chaired by VINCI's Chief Information Officer, ensures that the overall cybersecurity strategy is fully in line with the overall information systems strategy. It makes sure that the cybersecurity strategy is effectively implemented by the business lines.

Members: VINCI's Chief Information Officer, Chief Information Officers in the business line.

Cybersecurity committees in the business lines

Each business line can set up as many committees as it needs according to its context and organisation.

The following two committees are recommended for each business line:

Business line cybersecurity steering committee

A cybersecurity steering committee should be set up for each business line, chaired by its CISO and meeting every six months.

Its responsibilities include:

- validating the follow-up on the business line's action plan and defining and monitoring the resources and related budgets;
- providing feedback on cybersecurity incidents and major crises.

Business line cybersecurity operating committee

A cybersecurity operating committee should be set up for each business line, chaired by its CISO and meeting on a regular basis. It ensures the effective implementation of the operational action plan.

VINCI'S REFERENCE FRAMEWORK FOR CYBERSECURITY

The cybersecurity policy relies on a set of standard documents, ranging from the general to the specific, listed below:

STRATEGIC

Mandatory

Policies

They formally define the main objectives of cybersecurity and the related governance.

This set of documents includes:

- VINCI's general cybersecurity policy (this document);
- the cybersecurity policies for the business lines;
- The VINCI Group Guide for Users of Information Systems.

TACTICAL

Mandatory

Directives

They clarify the mandatory security rules for each domain of the information system.

Mandatory

Standards

They include the technical standards and a presentation of the mandatory tools in the Group's information systems.

Optional

Best practices

These are compilations of a set of behaviours and rules already applied in the Group that have produced satisfactory results.

OPERATIONAL

Adjustable

Procedures

They give details of the steps and the precautions to take or the methodologies to follow when applying security measures. These procedures often need to be adapted to the technological context of the information system.

These procedures include, among others:

- Group-wide procedures (for instance, the procedure to follow in the event of leakage of personal data);
- procedures for each designated role (for instance, IT project managers, developers, systems administrators);
- procedures for each technology (for instance, operating system, servers, firewall).

These documents are made available to all parties concerned on the VINCI intranet.

REAL SUCCESS IS THE SUCCESS YOU SHARE

November 2018 edition– Photo credits: Luc Benevello – Design: www.gcommeuneidee.com

VINCI
1, cours Ferdinand-de-Lesseps
F–92851 Rueil-Malmaison
Cedex FRANCE
Tel.: + 33 (0) 1 47 16 35 00
www.vinci.com