Information Systems Security Policy May 2019





Preface

The security of your data, in addition to being our core business, is our daily priority. We therefore dedicate significant resources to the maximum protection of our information systems as well as our data centres, in order to ensure even greater protection for you.

Building a long-lasting relationship of trust with our customers, by providing services of very high quality, is an essential objective for us. At a time when threats are increasingly potent and sophisticated, it is our duty to continue to protect the resources which are entrusted to us and to consolidate the services that we offer.

That is why Scaleway has set up a security procedure the objective of which is to obtain labels and certifications respected in the market which are, for you, a guarantee of quality and trust.

Our employees adhere to this procedure and actively contribute to it on a daily basis. As responsible individuals, they ensure that the security rules are known, understood and applied, in their area of involvement and within their remit. Ever vigilant, they are on constant alert during their various usages and uses of the information systems, in order to detect possible incidents and to adopt the appropriate behaviour when faced with a risk situation.

This Information Systems Security Policy is applicable, in respect of the subcontracting relations between Scaleway and its Customers, to the data that the Customer sends to Scaleway to this end.

Scaleway thanks you for putting your trust in us.

Arnaud De BERMINGHAM

CEO

Contents

<u>1</u>	Security and our employees	4
<u>2</u>	Asset management	4
<u>3</u>	Access management	4
<u>4</u>	<u>Documentation</u>	5
<u>5</u>	Physical security	5
<u>6</u>	Security of terminals	6
<u>7</u>	Management of subcontracting	6
<u>8</u>	Network security	6
<u>9</u>	Confidentiality and data encryption	6
<u>10</u>	Security of our websites	7
<u>11</u>	Data back-up	7
<u>12</u>	The management of security incidents	8
<u>13</u>	Business continuity	8
14	Ongoing improvement	R

This document is the property of ONLINE SAS. Any dissemination or reproduction, even partial and in any form whatsoever, without the express prior authorisation of a person authorised by ONLINE SAS is strictly forbidden. This document is solely for information purposes and has no contractual value as it stands. (ONLINE SAS 8, rue de la ville l'évêque 75008 PARIS)

1 Security and our employees

At Scaleway, learning and applying the security measures starts from the employees being hired, so that the culture of security is disseminated throughout the whole company. Each employee is aware of the threats to the information systems and therefore knows his/her responsibilities in relation to them. That allows him/her to assume a role of an ongoing contributor.

To that end, the company has introduced a charter for the proper use of IT resources. This is signed by each employee as soon as he/she joins Scaleway.

When they join, our employees receive a guide of good security practices and are made aware of the issues associated therewith through internal departments and numerous training sessions organised on a regular basis.

2 Asset management

Effectively guaranteeing the security of our information systems requires knowledge of security needs. That is why each asset - hardware, workstation, server, telephone, etc. - is included in a detailed inventory and is then classified with an owner who is linked to them.

A disposal procedure is formalised and implemented when an asset is withdrawn from the information system or disposed of.

3 Access management

One of the essential factors of the security of the Information System is the management of physical and logical access: this relies on effective processes allowing good management of identities, the ongoing updating thereof and robust two-factor authentication mechanisms.

Thus, each user accessing Scaleway's Information System is duly identified and authenticated. Each account is assigned to a single individual to guarantee traceability of access and actions.

The rights and authorisations given to users are defined according to their business profile and in accordance with the principles of least privilege and separation of powers to guarantee data confidentiality. Accounts are reviewed every 60 days to ensure the legitimacy of all of the accounts.

A separate password policy for user and administrator accounts including complexity rules is implemented when creating and modifying an account.

4 Documentation

Documenting the methodologies, processes and actions is essential to ensure their proper application.

The documentation is therefore regularly updated. It standardises the practices within Scaleway and is used and implemented at all levels of the company.

5 Physical security

At Scaleway, we actively implement physical security policies both in our data centres and in our premises.

A set of physical protection measures is implemented including the following:

- Video protection and anti-intrusion systems on all sites;
- A security airlock with single entry verification to guarantee the security of entry/exit flows;
- A unique access badge with a biometric fingerprint for each employee or visitor;
- Access control by active badges at all entrance and exit doors;
- An access and site management policy based on the profile of the employees and subcontractors;
- A security guard or receptionist or, failing that, ongoing monitoring by duly authorised company employees.

Each user of the Information System also contributes to physical security by complying with the good practices, such as shutting office doors, the "clean desk" policy, the locking of workstations during absences, the encryption of workstations by default, or the enhanced protection of sensitive documentation.

6 Security of terminals

Scaleway's workstations are all equipped with disk encryption by the operating system. Access to the workstation is only possible after a mandatory authentication phase (password or biometrics).

Mobile business equipment is also protected by biometrics. Our employees take all necessary precautions to protect their equipment, in order to best ensure the protection and security of personal data, in accordance with our security policy.

7 Management of subcontracting

All contracts with our subcontractors include applicable strict security requirements as well as means of checking compliance therewith.

The requirements that we have with our subcontractors are at least equivalent to our own internal security requirements, in order to respect our commitments concerning a high level of security of the information systems.

8 Network security

A network partitioning and confinement policy is implemented within Scaleway's networks. This partitioning is accompanied by a policy of internal and external filtering in order to combat malware.

The networks within Scaleway's Data Centres are redundant and allow it to be ensured that business is continued for customers and employees.

Also, remote access to Scaleway's information system is achieved via an encrypted and authenticated VPN.

9 Confidentiality and data encryption

Various encryption measures are implemented to ensure the confidentiality of the data hosted and processed.

Firstly, all of the storage of the workstations is encrypted by default, so as to guarantee that the information is inaccessible to unauthorised persons.

Then, you can control the storage of your content and choose the security status of your content and the data in transit. Scaleway provides you with encrypted and authenticated VPN tunnels.

Finally, the media containing the information are protected against unauthorised access by means of physical protection.

Scaleway never accesses or uses the data that you store other than in the cases expressly stipulated in the contract, on your documented instruction or if the applicable regulations require it to do so. In addition, your data is never sold to third parties.

10 Security of our websites

At Scaleway, we are aware of the various constant threats that websites are under. For this reason, we have taken the necessary security measures to guarantee the protection of the data processed by our sites.

Hence, we use the latest versions of the TLS protocol on all of our websites, ensuring that it is particularly effective on the pages processing personal data (e.g. registration forms, connection page, etc.). You are however solely responsible for the confidentiality and security of your logins to your console.

We have also introduced a policy relating to the use of tracers which we can place on the terminals of visitors in order to explain their purposes and their operation, in a fully transparent manner. We also ensure that the visitor can manage the use and the placement of these tracers.

Finally, all of the actions associated with user accounts are strictly reserved for a limited number of administrators, and are strictly limited to the requisite administration actions.

11 Data back-up

All of the applications, operating systems, events, configurations of the equipment and production data which deliver a function to the users (internal, customers, etc.) are backed up regularly. The frequency of the back-ups depends on the type, the sensitivity and the volume of the data.

Regardless of the data backed up and the type of back-ups, they are stored on dedicated servers.

Only the system and network administrators, and also the ISSM, can access the back-ups for legitimate reasons such as the management of incidents.

Finally, data recovery tests are carried out regularly by the system and network administrators on Scaleway's functional scope in order to ensure their correct functioning.

12 The management of security incidents

Security incidents are handled in accordance with a formalised, validated procedure known by all. This allows an appropriate response to be provided in the event of a major incident that might affect the security of the Information System or of the data of its users, agents or clients.

These procedures are regularly tested and updated to ensure their relevance and effectiveness at all times.

In addition, all users are obliged to report to the security teams, without delay, any act that may represent an actual or suspected breach of the security rules.

13 Business continuity

The continuity of the Information System is assured thanks to a set of measures, including:

- The redundancy of primary infrastructure equipment (air conditioning, hardware, incoming electrical lines, generator sets, power supplies to the racks, etc.);
- Local technical support with technicians onsite or on call, allowing rapid intervention on the equipment or infrastructure in the event of an incident;
- A formalised and regularly tested business continuity and recovery plan in order to reduce downtime due to an incident as much as possible;

14 Ongoing improvement

At Scaleway, the security measures and practices are reassessed periodically and regularly, in order to take account of four important elements:

- a) Changes in the threats;
- b) Good risk coverage;
- c) Regulatory changes;
- d) Exhaustive coverage of the scope.

(Strategic, steering and operational) dashboard systems are also implemented to allow the monitoring of, in particular, the level of application of the rules, the level of security, the incidents and the effectiveness of the measures and the resources.

Faced with the ongoing changes in the risks that the information systems might be under, Scaleway has implemented effective monitoring that allows, in particular, new threats and new security standards to be detected.

Regular internal or external audits also allow Scaleway to ensure the effectiveness and the performance of its systems at all times and that they are updated where applicable.
