hector

Security Insurance Plan

Asset Management of Hector Online Applications

hector

Table of Content

hector

1. Evolution of Document

Publication Date	Author
27/10/2021	J. Montambeault

Distribution

Document distributed to Hector Inc. customers and potential customers

2. Introduction

Objective

The Security Insurance Plan, hereafter designated in this document as SIP, describes Hector Inc. commitment to data and application security that are hosted on their provider's platform, Vultr. Holdings.

Perimeter

SIP applies to all the services supplied to our clients and are mainly shown hereafter:

- Asset management application developed by Hector (SaaS mode)
- API (Application Programming Interface)
- Mobile Application available both in the Apple and Google Play Stores
- External backups (SaaS mode)
- Activity Recovery Plan (ARP)
- Server and application hosting

The Teams

Hector and its team will supply to their clients hosting services and applications through its SaaS infrastructure. The teams are permanent employees of the company. The main activities of the team are as follows:

- Manage and update the infrastructure.
- Implement new hosts for SaaS applications sold to our clients.
- Ensuring operational and administration services.
- Ensuring technical assistance to our clients.

Reference Documents

GSC : General Service Conditions
Particular conditions such as:

- Particular Hosting Conditions
- Particular Conditions with regards to SaaS Services
- Particular Service Conditions

The complete set of documents are available on our website: hectorassetmanager.com/

Rules and regulations regarding the Protection of Personal Data:

- Act n°78- 17 dated January 6, 1978 regarding computer science, files and liberties, modified by Act n° 2018-493 dated June 20, 2018.
- General Rules on Data Protection (RGPD)

3. Challenges and Objectives

Challenges

The security of the host provider and the Hector information systems are an essential component for the protection of Hector's interests as well as those of its clients.

Therefore, it is imperative that a Security Policy be in place for the Information Systems, and that this policy takes into consideration the main risks incurred and identified:

- Risk of unavailability of information, applications and processing systems.
- Risk of disclosure and/or loss of confidentiality, whether accidental or voluntary, of the information given to us by our clients for which we act as a subcontractor.
- Risk of alterations or loss of integrity that our clients may experience due to a loss of information.

The objectives for the implementation of the System Information Security Policy are:

- Improve and formalize the security management of our host provider.
- Provide an extension of actual services by proposing host services on a public Cloud, for example, Azure offered by Microsoft already certified ISO 27001.
- Extend all good practices to services provided by Hector.
- Ensure that Hector respects its legal obligations regarding its management of Personal Data (Act on Computer and Liberties, RGPD), and that Hector be able to provide evidence thereof to its clients to whom they intervene as subcontractor.
- Create a security culture within the Hector team and extend this culture to its vendors and customers.

4. Risk Management

The Hector management team ensures that the risks to any information security breach that may result in an unacceptable service disruption for its customers be continuously managed.

The selection of the host provider, Vultr, for hosting the clients' data was done following a deep analysis of service providers, certification of their data centers, that their data centers be located at several key geographical locations, and that their security culture be exceptional.

This risk analysis gave way to the implementation of an evolving action plan of their security measures.

5. Information System Security Policy

In order to conform to its regulatory obligations, to improve its processes, to permanently integrate the aspect of information security, and thereby improving the practices of all technical teams, Hector Inc. updates its Security Policy (PSSI) annually.

This policy was implemented in 2019 when the company was founded and is regularly reviewed based on the security standards of ISO 27001 and ISO 27002, and is completely integrated in the company.

A Delegate for Data Protection (hereafter designated DDP in the document hereafter) has been named. This person is equally responsible for quality and the security of the company. This person's mission is to ensure that PSSI respects their legal obligations regarding the Protection of Personal Data.

The PSSI is distributed to everyone involved and Hector Inc. implements all necessary training and information that is required for comprehension purposes, for its implementation and for its compliance.

The PSSI is an internal and confidential document of Hector Inc. The Security Insurance Plan (SIP) includes the information in PSSI, is communicable to clients, thereby facilitating its being read and understood.

6. Information Security Organization

Organization

Every employee has a job description that includes their mission, their position within Hector Inc., their main activities and the knowledge and know-how that they must master in order to properly perform their missions.

The security is reviewed:

- At a minimum once a year during a strategic management review dedicated to security by the management committee of the company.
- At a minimum, once a month at an operational level.

The department heads are responsible for conformity to the actual PSSI by their teams.

Supervision

Hector Inc. ensures that their providers are qualified in security, and participates regularly in demonstrations on the evolution of regulations, techniques, organizations and products.

Risk Management of Projects

The project methodology adopted by Hector Inc. considers the notion of risk in all new projects.

Mobility and Work at Home

Access to Hector Inc. Information Systems is allowed solely on materials that are owned by the company, even when working remotely from home.

7. Security of Human Resources

Hiring

A formal orientation program for ‘new hires’ is instrumental in integrating all new employees. Access to information and applications may evolve according to the integration status of the employee (minimum duration of presence on site, trial period ended, etc.).

Confidentiality

Each employee must sign a confidentiality and non-disclosure agreement included in their work contract.

Each employee acquires knowledge of the IT charter, signs, complies to and makes others comply with the charter. This charter also references confidentiality obligations, and defines the good use of the computer and encryption resources at their disposal.

Security Awareness

The formal orientation program of each new collaborator provides a program of security awareness. Awareness sessions are organized annually, either through attendance or by webinar.

Skills and Training

Management of skills by the Hector management team helps in identifying all training needs required.

Department heads define the training needs for their teams, advise HR and are validated and included in an annual training plan.

Departures

A formal departure program helps to implement the actions to be taken by HR and required by the collaborator upon their departure; in particular, the closing of their access rights to different accounts and sources to which they were allowed.

8. Asset Management

Asset inventory and identification

All assets of Hector Inc. employees are identified and inventoried in the asset management system of the company.

Removable Support Management

A removable support system (USB devices) are not used during the administration and operation of the hosts provided to customers. The technical teams do not have access to this type of support and cannot introduce unauthorized software on servers hosting customer data.

Asset disposal

Any physical support of data is destroyed before its disposal. The only exception is sending a hard disk to a constructor as part of managing any material under warranty. In that case, the constructor commits to physically disposing of the material.

9. Access Control

Password Policy

Each user is identified by a unique username and strong password.

- The password policy for users of the host providers is the following: Personalization by the user during their first logon to a production environment.
- Maximum size: 8 characters
- Complexity: Letters, numbers and symbols
- Change frequency: Every 6 months
- Cannot reuse preceding 5 passwords
- Lockdown after 5 erroneous attempts

Passwords are personal and confidential, therefore, cannot be stored by the technical team. If, for any reason whatsoever, a technical user needs to access the password of a user, the user must change the password before communicating it to the technician, and would then be required to reinitialize it before their next connection. The administration accounts follow the same rules as the users, with the exception that the minimum size of the password is 16 characters. These passwords are stored in a secured and encrypted database.

Access Rights Management

Permanent members of the team have permanent access accounts. The current administration of host environments is done by the infrastructure team through intermediary administration accounts with limited rights. Access by other technical personnel is authorized only for the length of time of the intended assignment or intervention.

Review of Access Rights

Administration access rights for all of Hector Inc. Information Systems are reviewed at least once a year.

10. Cryptography

Data Transfer

All data transfer towards a host provider is done through VPN links. If confidential data must be transferred to a removable domain, as an example by email, this data must be encrypted to conform to the rules in effect at the time.

Encryption

Technical teams use encryption software AES256.

Certificates

Certificates used by technical teams come from public and known certificate authorities.

Nomadic Workstations

The hard disks of technical teams' nomadic workstations are encrypted.

11. Physical and Environment Security

Location

Hector Inc. data centers are located in the following places:

- Toronto, Canada
- New Jersey, United States
- Paris, France

Certifications of data centers

Location	SOC TYPE I	SOC TYPE II	ISO 27001	PCI-DSS
Toronto	Yes	Yes	Yes	Yes
New Jersey	Yes	Yes	Yes	Yes
Paris	Awaiting Certification	Awaiting Certification	Yes	Yes

https://www.vultr.com/resources/faq/#datacenter_compliance

12. Operational Security

Operational Procedures

Hector documents all its activities; operational procedures are documented, updated and regularly audited.

Malware

Hector Inc. does not have an internal computer network. All work executed by its employees is done through the Google Workspace Cloud suite. Access to Google Workspace is secured by security practices described in the Access Control section. Each workstation is equipped with a software suite against malware. The availability of updates is verified daily, are automatically uploaded and distributed to the equipment.

Supervision and the centralized administration console immediately detect any anomalies (updates not distributed, infections, etc.).

Backups

Client data on SaaS hosts are backed up every day with a retention time of 7 to 30 days (or longer) as per their individual service plan.

The virtual servers of host environments are backed up every day with a retention period of 3 months. All backups are duplicated daily on a different cloud provider than the host provider.

Recovery Tests

Recovery tests are performed daily to guarantee that no faults have been introduced to the backup system.

Supervision

Services, communication methods and services are constantly monitored, and alerts are positioned so that the teams are informed immediately of any potential anomaly, or any situation that may lead to service degradation.

System Update Management

Services: Critical and security updates are distributed on a sample pilot equipment as soon as they are available, and are then distributed to all equipment if no anomalies have been detected during a period of 1 week.

Application Update Management

Critical and security updates are distributed as soon as they are validated in a testing environment.

The company carries out 3 to 4 updates of the software per year after extensive testing and quality control procedures.

13. Communication Security

Technical Architecture

Administration and management: A dedicated link is used by Hector technical teams for all interventions on the host provider platform; access to this link is allowed only by people skilled on MAC address and IP address. In the case of a rupture or unavailability, it may be accessed via Internet through the Vultr platform.

Firewall

All access to host provider and SaaS applications are through physical and software firewalls.

Intrusion Detection

All access connections to the platform are analyzed to identify and block abnormal flow and malware programs.

Intrusion tests are done every month to detect any vulnerabilities. Critical vulnerabilities are treated on the same workday of their detection. Severe vulnerabilities are repaired during the week following their detection.

14. IS Acquisitions, Development and Maintenance

Development Policy

Development activities conform to V cycles or Agile methodologies that are used by Hector teams.

All new versions, be they fixes, new developments or updates of a version, have been tested and validated before being added to the SaaS environment.

A rollback phase is enacted should the least malfunction be detected after an update.

15. Relation with Providers

Subcontractors are brought in to intervene on a host provider and may come:

- From the owner of the data centers

Relations between these subcontractors and Hector conform to the requirements of RGPD, and take into consideration all security aspects.

All subcontractor interventions are tracked and must comply with procedures, especially those with regards to access rights assignments.

16. Management of Information Security Incidents

Security Incidents

Every SI actor and host provider, user or administrator, Hector Inc. or subcontractor, Client, is aware of the importance of signaling all real or suspected incidents. This includes theft of computer methods or data support.

Signaling and registering incidents are systematic. Clients do it using a Hector Inc. ticketing tool, internal users follow a procedure in place. This procedure describes increases and people to alert according to the gravity of the incident.

Statistical data regarding incident management are integrated in the SI security dashboard.

A violation-type incident of Personal Data must conform to RGPD obligations; it may require notification to the authorities.

Crisis Management

The crisis management plan integrates computer risks as well as susceptible risks to the IS or host provider.

17. Conformance Management

ISO 27001: Hector data centers are certified for security management according to the standards of ISO 27001 and ISO 27002, suppliers of host services and SaaS application, and for the provision of services to all the clients.

Personal Data: The Delegate for the Protection of Personal Data is the Hector Inc. guarantor of conformance to their obligations. He may be reached at the following address: rgpd@hectorassetmanager.com.