Information Technology

Corporate Security directives

IT Department
Version 1.1
January 2014

Document history

Version	Date	Author	Modification description
1.0	05.02.2014	M.Gaudreau	Draft
1.1	13.03.2014	M.Gaudreau	Added comments following steering meeting
1.2	07.05.2014	M.Gaudreau	Added comments referring to deleted email

Document status & approbation

Status	Approbation
Approved	Name : Antoine Camarda Jean-Guy Cadorette Jean-Pierre Azzopardi
	Function: Steering committee members
	Signature:
	Date : March 31, 2014

Distribution list

A	Cc:
All employees	

INDEX

Initials _____

1. MESSAGE FROM THE PRESIDENT

Technology and information assets are critical to the Helios Group's operations and its business units. They must be subject to appropriate use and adequate protection. The Helios Group holds personal information that have a legal, administrative or economic value. Their use must be regulated in order to avoid incidents that could have negative consequences for both the employee and the organization as well for people who benefit from the services offered by it. This Directive aims to ensure compliance with laws, regulations or other normative acts regarding the use and treatment of information and the use of information technology and telecommunications by the employees of the Helios group. More specifically, the organization seeks to ensure respect for individual privacy, including confidentiality of information of a personal nature relating to customers and employees in order to protect information assets held by the organization according to their sensitivity.

The Helios Group requires any employee who uses the systems and information assets of the organization or who has access to information, to comply with the provisions of this Directive

Initials _____

1.1 Introduction

The information is more than ever at the heart of solutions to optimize business processes. In return, information security may be compromised if preventive and concrete actions are not systematically undertaken during the development of e-business solutions or in the adoption of document management practices and their evolution all throughout their life cycles. To mention only the leakage of critical information on a major project, fraudulent accounting transaction using a computer system or a cyberspace attack jeopardizing the operations of the Helios group. The risks are present. These business risks with regard to information security may be legal, strategic or financial, can tarnish the reputation of the Helios Group and undermine the trust model of our customers to the company.

The importance of protecting the information for the Helios group justifies the establishment of an information security management program in order to maintain the levels of risk in accordance with the expectations of management of the company. This program should also consider the organizational, human dimensions, legal, financial and technological.

An effective information security program requires coordination and concrete integrated action concretely from the top of the hierarchy down. The formal endorsement, promotion, as well as the support of the senior management are prerequisites for the success of the information security program commitment. Thus, in this context, this Directive is developed to support a program of information security in the Helios Group. This Directive confirms the Group's commitment and demonstrates the importance of the protection of its information assets.

1.2 Objective

State the corporate directive of the Helios group to ensure the integrity, confidentiality, availability of information and the protection of its information assets. This directive also aims to ensure that the Helios group will be able to deal with technical or human error, malicious acts, as well as sinister.

1.3 Definition

Information: information in any form (written, alphanumeric, numeric, audio, graphic, pictorial, photographic, symbolic, etc...), on any media or communication channel wired and non-wired.

Document: organic recorded information, regardless of media support.

Communication and Information technology systems : considered as such, including database, application, program, software, computer hardware or telecommunications equipment, a virtual space, a computer, printer, fax machine, telephone, radio transmitter, a scanner, etc..

Information assets: any information, document, system and information technology or communication.

Responsible for an informational asset: Manager of Helios group acting as owner or trustee of an information asset.

1.4 General principles

The directive seeks to define a set of measures designed to meet the security of information collected, held or used in the Helios Group. In addition to protecting the access, processing, use and transmission of information, the general principles governing this Directive aim to ensure that:

- The Helios group can, through its authorized as hereinafter defined representative to audit the information residing or transmitted over the network or its equipment and, at any time and in its sole discretion;
- The IT department is responsible for all mechanisms to ensure the security of information residing in an electronic format;
- The IT be assessed by an internal process on a regular basis, department directives and security mechanisms of the Helios group versus security best practices;
- Only authorized personnel can access and reasonably use the information necessary for its work, according to the specific permissions granted;
- Staff does not disclose the information without the written authorization of the person to whom such disclosure or employees under a confidentiality agreement (except as provided in the Act on the Protection of Personal Information in the Private Sector, RSQ , c P-39.1, which verification shall be made to the corporate Secretary prior to any unauthorized disclosure by the person).;
- Confidential information available to staff should be used only for business purposes and for the benefit of the Helios group;
- The use of the infrastructure should be used only for authorized purposes in accordance with this directive;
- Let the established mechanisms for compliance and sanctions for breaches of the Directive.

1.5 Fields of application

This directive regulates any information related to all activities of the Helios Group and applies to all units.

Any third party whose services are required by the Helios group and having access to confidential information, is also subject to the Directive and it must agree in writing to abide by the standards, procedures and security directives related to it or that may arise.

1.6 Regulatory Framework

Some aspects of information security are governed in particular by:

- The Act respecting the legal framework for information technology (RSQ, chapter C-1.1);
- Act respecting access to documents held by public bodies and the Protection of personal information (RSQ, chapter A-2.1);
- The Law on Archives (RSQ, chapter A-1.21);
- The Canadian Act Copyright Act (RSC, chapter C-42);
- The Civil Code of Québec;
- The Evidence Act (L.R.C., chapter C-5);
- The Act respecting the Criminal Law (LRC 1985, chapter C-46);
- The Civil Protection Act (RSQ, chapter S-2.3).

1.7 Detailed Principles

Rules to be followed and measures to be taken

Responsibilities of employees and managers

Helios group staff is responsible, as part of its duties and functions to effectively manage access, processing, use and protection of information, depending on its nature, signed agreements and its value, in order to ensure confidentiality.

Managers responsible for units that collect, produce, possess or use the information are responsible for providing the authorizations provided for the access, processing and use of such information and shall be accountable.

IT Department Role

Any amendment to the Directive, any security directive and procedures resulting standards shall, prior to their implementation, have been reviewed and approved by the IT department.
The IT department will ensure the level of security, its maintenance and updating it according to best practices in such matters.

Limitation in the collection of information

In cases where the nature of the information is personal, only the information required for carrying out the activities of the Helios Group, and for reasonable purposes, should be collected from the person or, if the collection is made with through a third party, with the permission of the person, all in accordance with the provisions of the Act on the Protection of personal Information in the private Sector, RSQ, c. P-39.1.

Classification and description

Information should be classified (classification in appendix) according to its confidentiality, availability and duration of its useful life (with a retention schedule).

Security measures

Security measures (eg. Encryption, access control, etc.) Must be taken to protect the confidentiality of the information.

Security measures (eg, detection of computer viruses, manual or electronic signature authentication, audit trails) must be taken to preserve the integrity and authenticity of information, and to confirm or refute the origin of information.

Security measures (eg, copies, locked office and filing cabinets, put in external vault, IT continuity plans and disaster recovery plans for information technology) must be taken to ensure the availability of information in case major failure or disaster.

Security measures must be adapted to the level of classification of information.

Retention of Information

The information must be retained as long as necessary, depending on the operational needs of the business and regulatory frameworks and / or applicable legal rules.

The information that does not have to be stored must be destroyed according to the procedures established in accordance with the rules of confidentiality.

Initials _____

1.8 Monitoring Mechanism

This Directive is issued to all units. The directions of these units will monitor the effectiveness of the Directive in the light of their specific mission. To this end, they will implement the following mechanisms:

- Regular checking of compliance specified in the directive and implementation frames thereunder, on a schedule that takes into account issues to be addressed as a priority. Reports on compliance with the rules laid down in the directive will be issued by the department managers responsible for the affected units on a regular basis (implementation planned 2014).
- Annual review of frameworks and tools necessary for the application of this Directive to ensure they are adequate and relevant according to the changing operational environment, technological, legal, etc..
- Permanent information and Training programs about the Directive to ensure frames resulting.
- Consolidation and coordination of monitoring of the Directive. All administrative units must ensure the implementation of this Directive and provide the information necessary to monitor. Monitoring mechanisms aimed at the implementation and compliance with the rules and principles of this Directive.

2. PRINCIPLES OF IT SECURITY

2.1 Responsibilities

Security Officer (IT Director)

The officer shall ensure that the directives are known and respected.
The officer must ensure that everyone knows their responsibilities.

Administrators

Administrators must ensure to never disclose combinations and access they have.
The administrators are responsible for maintaining access.
The administrators are responsible for monitoring access violations.
Administrators must enforce the law on the confidentiality of information.

Users

Users must make sure never to divulge passwords they have.

Head of Maintenance (Longueuil site)

The Head of Maintenance shall provide a resource to change the server room door combination when asked.

Responsible for an application (Power users)

Managers must ensure that once a year access to applications are valid.

2.2 Password

The password is one of the main ways to ensure security of access to systems and to information within the organization. As a result, basic precautions apply:

- Use a password of at least eight characters, consisting of uppercase and lowercase letters, at least one number and one special character;
- Avoid using a dictionary word or a word that resembles the name of the organization, service, software, system or employee;
- Do not show or write the password on a piece of paper at the sight of others;
- Do not allow a user to log with someone else ID of the employee unless formally authorized by their superior (the employee is responsible for all actions performed with their username and password).;
- Lock the workstation when leaving it for a specified period of time or mementarily;
- Change the password at regular intervals (maximum six months) or when the system demand is highly recommended;
- Do not disclose your passwords at any time.

Enter your password each time you connect to a secure site is highly recommended. The "Remember my password" available in browsers or in some Web pages function should not be used.

Your username is kept in several electronic transactions for auditing purposes: it is your electronic signature. Depending on how many services you use, you may have multiple user names and passwords to remember. The password is mandatory for all users.

For users who use a remote control software to take control of a PC remotely through <Log me in, PC Anywhere> or any other similar software, we ask you to use a complex password.

To do this, use a paraphrase easy to remember. Example; 'I've joined the Helios Group in January 2014> Taking the first letter of each word, the first in capital letter and before the number you add your special character.

This will result in: Ijthgij@2014

2.3 Voicemail

No password expiration.

2.4 Computer (PC or laptop)

Customization (installation of software or other) can be performed by the user provided that it is properly licensed and it is related to his work. It is strongly recommended to coordinate with the IT department.
Thus, the IT sector is sure to keep legal copies of all software installed. In addition, if you must replace the workstation if it is defective, we will have all the software in hand to rebuild the new workstation.
Make sure you lock your workstation if you are absent. A work station unlocked and unattended provides access to all your data without difficulty.
The PC must be protected by a session process. The user must set session with Windows servers for access to IT services.
The PC must be protected by a corporate antivirus that also detects «spyware / malware."
PCs receive security updates every week or as needed.

2.5 Backup

A backup copy of your files on enterprise servers and emails is taken every night. The latest version of the files is saved. Deleted e-mails can be recover for a maxomum period of 14 days.

The latest version of your files is saved as long as the option "files history" is activated and used with "OneDrive".

Note that there is no backup copy of the files on your own workstation, or your C drive unless previously agreed with the TI department.

2.6 Disaster recovery plan

The disaster recovery plan for IT covers all computer and telephone equipment located in facilities located in Longueuil and Montreal areas. It covers the following three crises:

- Server room unreachable (immediate recovery);
- Equipment breakdown (maximum recovery time is one week);
- Total lost of the server room (recovery in one week).

2.7 Remote access connection

Access via Citrix or VPN must be controlled by a level of security, it is controlled by the Windows network security.

Strong encryption SSL (128-bit) is used to protect the confidentiality of information between the client and the VPN or Citrix server.

2.8 Remote VPN connections (Internet access through a wireless Internet at the hotel or the airport)

Access via a wireless network in airports and hotels are not protected by a firewall and therefore represent a security risk. The user is exposed to an intrusion of his laptop and, therefore, the possibility to provide access through their laptop to access the VPN. A potential risk is the takeover of the laptop without authorization and thereby to have access to all your applications at the Helios group.

The laptop must be protected by a firewall when wireless Internet is used.

2.9 E-mails received from the Internet that are intercepted and destroyed

As a security measure, some emails are intercepted and destroyed at the reception:

- emails containing viruses and detected by our corporate anti-virus;
- emails from a known site recognize for sending spam;
- emails from an unknown sender (sender who was not identified);
- e-mails with a bad address (destination unknown).

The recipient of the email is notified if the email was intercepted and destroyed.

2.10 Personal use of disk space, email and Internet

RATIONALE

This Directive aims to establish rules for the use by employees of the Helios group email (internal and external) and the Internet. Employees are committed and willing to respect and abide by the rules set out in this document for their use of electronic mail and the Internet.

DIRECTIVES

1. The Helios Group holds the exclusive property of electronic communication systems that are available to employees as well as the information attached to it and that it can containe. A record of websites visited by each employee is kept and maintained on a daily basis by the IT team.

2. Access to and use of email and / or the Internet will be allowed and granted to any employee whose work and functions within the company justify the use of such tools and resources. Any request for access and use is processed by the IT group on a case by case basis and must be authorized by the directors of sector stakeholders. This Directive does not cover installation, access or use of email or the Internet from the employee's home. Any expenditure incurred by an employee related to the installation of Internet access at home will not be reimbursed by the Helios group, unless otherwise stated.

3. The use of electronic mail and the Internet is a communication tool available to employees for their work.

4. However, personal use of e-mail and Internet is tolerated as well as the use of the business phone for personal use as long as the use is reasonable and does not prevent normal work performance of the employee and he shall be able to perform the assigned tasks.

5. Any use by an employee of e-mail and the Internet for personal use should not interfere with the proper functioning of current operations of the company. The employee has the responsibility to use the business resources effectively, without exposing the Helios Group and its systems to undue delays, congestion or outages or situations that could undermine its reputation or the rights of others.

6. Because e-mail and Internet are primarily intended to serve the interests and to perform work or services for the benefit of Helios group, the employee must be aware that the Helios Group can not ensure or guarantee privacy or private nature of the communications passing through its systems. However, the Helios group will attempt, to the extent possible, to respect the right to privacy of any employee making personal use of email and Internet, within the limits and conditions set out in this Directive.

7. The employee has a duty to use email or the Internet in the respect for the dignity of others and to contribute to maintaining a workplace that is free from discrimination and harassment. Thus, any use of electronic mail and the Internet involving or relating to any illegal or unlawful activities or sexual or pornographic connotation, in all its forms, not consistent with the Directive of the Helios group or containing messages of intolerance, threats, hatred or defamatory, is strictly prohibited.

8. The Helios Group reserves the right at its discretion to block access to certain websites it considers non-conforming or do not respect the rules of this Directive or hindrance, heavier or slows unduly systems (eg. sites distributing music).

9. Due to network congestion and the growing user and system data stored in its number, the employee must restrict to a minimum the files of a personal nature stored on the network. All personal email received, especially with an attached file, should not be retained by the employee in the network and should be deleted after reading.

10. Similarly, the transmission or reception of jokes through e-mail and the Internet should be treated the same as a communication of a personal nature and, therefore, be made in compliance with the rules of this Directive. They should not be kept or stored in the network of the Helios Group and will be destroyed after reading.

11. Should the Helios group finds misuse that is not conforme under this Directive, the Helios Group reserves the right, where appropriate, to verify the use made by any employee of the email and Internet use as well as addresses or websites visited. In circumstances where an employee abusing this privilege, the Helios group will take corrective action it considers appropriate against him.

12. The internal e-mail of Helios Group is a private system. However, the external mail (via the Internet) can not be considered private and does not protect the confidentiality of information they conveyed. Since it is not illegal to access the data provided by others on the Internet, the employee must use this mode of communication with the necessary precautions and use. For example, the message transmitted over the Internet can be intercepted by someone outside the company as well as the owner of a visited website can easily identify the origin of a consultation.

13. The department of information technology has deployed a corporate antivirus software and maintains it. However, antivirus software is always one step behind the virus writers. It is therefore important to be wary of anything that is downloaded from the Internet, especially files attached to emails. The problems usually start when "double-click" on them to open attached files. So never do this lightly. The Helios group therefore requires from its employees to be particularly vigilant. Please refer to the help desk service when detecting any virus or suspicious file.

14. Any breach of this directive may result in disciplinary action up to dismissal.

2.11 USB stick or other external media

It is important to protect all the important information that is on your USB key. Especially confidential one. You can do this through encryption. The information will then be unusable if the device is stolen or lost. IT service will tell how to do this.

2.12 PC and portable for remote people

- The PC will not open direct session on the network of the Helios Group. They do this through a local session.
- The PC must be protected by a process of local session.
- The PC must be protected by a corporate antivirus that also detects "spyware / malware."
- The update of the virus definition and Windows security should be automatic.
- When connecting to the Internet, Windows Firewall must be enabled.

2.13 PC and portable

- Laptops must be protected by a session process.
- The user must use a Windows server session for accessing IT services.
- Customization and installation of software on portable should be reserved for IT specialist.
- Laptop have to be protected by a corporate antivirus which detects both spyware and malware.
- Laptop goes off session (screen saver mode) after 30 minutes.

ANNEX A

Classification of information accessibility

Classification	Description	Accessibility
Public	Is considered public information which is public domain.	Without restriction
Confidentiel	Is considered confidential, any information not known to the public on the Helios Group, its activities, its employees, suppliers, partners, etc... Any sensitive information that, if it were to be disclosed without authorization, could prejudice the interests of the Helios group (as well as those of its employees, suppliers or partners). The following categories are examples of confidential information. Note that the categories and examples they contain do not constitute an exhaustive list. **Confidential personal information** • Social insurance number, phone number, bank account number, credit, date of birth, address, age, gender, personal email address, etc. • Marital status, medical history, etc... (Of an employee). • All information block to identify an individual precisely (employee). **Third party confidential information entrusted to the company** • Commercial Financial Information, scientific, technical or trade union confidential provided by a third party usually treated by a third party as confidential. **Information affecting the company** • Information from commercial contracts. • Information on contracts with partners and suppliers. • Information regarding investment strategies and competition. • Mandate or negotiating strategy of collective agreement. • Transaction or proposed transaction in respect of goods, services or works. • Legal Opinions. • Mémoires or proceedings of any decision-making body. • Advice or recommendations of staff, consultant or other organization. • Test for the comparative assessment of knowledge, skills or experience of a person.	Accessible to staff who obtained explicit permission to access

Initials _____

	• Information obtained by a person who, under the law, is responsible for the prevention, detection or repression of crime or statutory offenses. • Information in the guise of a prohibited communication or order of non-publication, non-disclosure or non-disclosure. • Information on the security features of the company. • Information about anticipated financial results of the company.	

ANNEX B

Classification of the availability of information

Classification	Description	Accessibility
Critical	Information availability is **critical** to the mission of the company and whose unavailability is tolerable only for a short time.	48 hours
Essentiel	Information availability is **critical** to the company's business and whose unavailability is tolerable only for a short time.	Between 3 to 7 days
Non essentiel	Information whose availability is **not essential** to the activities of the enterprise and the non-availability is tolerable for an extended period.	More than 7 days

Employee signature	
Initial each pages	Name :
	Fonction :
	Signature :
	Date :