INFORMATION SECURITY POLICY AND ASSET USAGE

BH COMPLIANCE

Policy Owner ("Owner")	Ramón Montero – Chief Operational Officer (COO) ramon.montero@bh-compliance.com
Recipients of this policy (the "Policy")	All users of BH Compliance's information systems and communications, including employees, contractors, and suppliers (collectively, the "Users")
Objectives	The purpose of the Policy is to define the standards to safeguard the information of BH Compliance and its Clients against unauthorized use and disclosure.
Implementation Date	April 2023
Version	6
Related Documents	Internal Regulations of Standards, Policies, and Procedures Employment Contract (employees) Service Agreement (suppliers)

TABLE OF CONTENTS

1. GENERAL ASPECTS

1.1. INTRODUCTION

BH Compliance is aware that information is one of its most important assets, as well as that of its Clients, and that, at the same time, it is exposed to risks and threats that can arise both from within and outside the company.

1.2. OBJECTIVES

This Policy aims to establish the general guidelines for the definition, implementation, handling, and control of the logical and physical security of information assets within the company, to protect their confidentiality, integrity, and ensure their availability.

In particular, the Policy seeks to:

- Protect BH Compliance's information assets and, especially, Client information, as well as ensure its proper use, regardless of the medium in which it is stored (paper or electronic).
- Prevent unauthorized access to BH Compliance's information systems.
- Protect the use of devices used to access BH Compliance's information assets.
- Promote and raise awareness among the recipients of this Policy about BH Compliance's responsibility, as an organization, to protect and properly use information, as well as all BH Compliance information assets.

1.3. SCOPE

The Policy applies to the use of all information assets, both tangible and intangible, of BH Compliance, which includes not only the information of BH Compliance and its Clients but also all equipment, devices, networks, technology, and services through which such information is accessed or processed, that are:

- Accessed at or from BH Compliance's facilities; • Accessed remotely, from any source or platform;
- Accessed through the use of BH Compliance devices or devices controlled by BH Compliance;
- Used in a way that identifies the person accessing BH Compliance's information assets.

Information security is everyone's responsibility. Compliance with this Policy by BH Compliance Users is essential for the governance, security, and management of information assets.

1.4. REGULATORY FRAMEWORK

The following non-exhaustive regulations impact the scope of information security and this Policy:

- Law No. 20.393 on criminal liability of legal entities
- Law No. 21.459 on cybercrimes
- Law No. 19.628 on the protection of privacy
- Law No. 19.039 on industrial property
- Law No. 17.336 on intellectual property
- Law No. 19.799 on electronic documents, electronic signatures, and certification services for such signatures

2. DEFINITIONS

A) Information Asset: Any information that holds value for BH Compliance and/or its Clients, regardless of the medium in which it is stored, as well as all devices, equipment, software, technology, networks, services, media, procedures, and other tangible or intangible assets that process, store, maintain, protect, or control access to information within the organization.

B) Confidentiality: The property of information that ensures it is only disclosed to authorized individuals or processes.

C) Clients: Clients of BH Compliance.

D) Availability: The property of information that ensures it is accessible in a timely manner as required by those authorized to access it.

E) Responsible Party: The person in charge of ensuring compliance with this Policy and fulfilling the obligations established herein.

F) Information Security Event: The occurrence of a state or situation that constitutes or suggests a current or potential violation of the information security policy or a failure in security controls.

G) Information Security Incident: One or more unexpected or undesired information security events that, with certainty or significant probability, compromise BH Compliance's operations and/or threaten the security of its information assets. This includes any unauthorized access, attempted access, acquisition, disclosure, destruction, loss, or use of BH Compliance’s or its Clients’ information, as well as the reasonable suspicion of such events occurring. Additionally, an Information Security Incident includes any cyber attack generated from BH Compliance’s systems to any external system that has the potential to be classified as a cybercrime under Law 21.459.

H) Integrity: The property of information that requires protecting its accuracy, ensuring it can only be modified or deleted by authorized individuals or processes.

3. GENERAL GUIDELINES FOR INFORMATION SECURITY

3.1. INFORMATION STORAGE

Information assets must be stored in the repositories designated by BH Compliance, whether on-premise or in the cloud. Centralized repositories will be preferred whenever necessary and feasible, in accordance with the company's operations and resources.

3.2. INFORMATION CLASSIFICATION

Information at BH Compliance is classified according to this table.

If you are unsure whether certain information is confidential or not, it should be assumed to be confidential.

Type of Information	Description	Examples
Public	This information is available to anyone.	Information available on websites. Publications. Articles.
Internal	Information that can be used by all employees of BH Compliance. This information may be provided to third parties, with prior authorization in accordance with this Policy.	Security Policy. General use policies and/or procedures. Internal communications
Confidential	This information has been disclosed to certain individuals at BH Compliance. Only those who need access to the confidential information due to their roles and are subject to confidentiality obligations will have access. It cannot be disclosed to third parties unless with prior written, specific authorization, and in accordance with this Policy.	All information about or prepared for Clients. Any information containing personal data. Human Resources information. Operational information of the BH Compliance business.

3.3. ACCESS TO INFORMATION

Access to information must be restricted, always following the information classification established in section 3.2.

Users may not extract information from BH Compliance's systems, nor store it on their personal devices, unless they have prior written authorization from the responsible party and the corresponding client. Such request and authorization will be issued via an email directed to the responsible party at the email address ramon.montero@bh-compliance.com. Then, the authorization will be granted solely to fulfill the purpose that motivated the User's request and will be valid only for the time necessary to fulfill it. Finally, once this authorization is obtained, the information must be safeguarded with the necessary security measures.

Users may only provide internal or confidential information to third parties in the following cases:

A) With prior written authorization from the owner or controller of the information (e.g., the client);

B) To third parties who require the information strictly within the context of the advisory for which BH Compliance was hired and to proceed with it;

C) To third parties who require the information to provide the services that BH Compliance has contracted; or

D) Existence of a legal obligation. In this case, the User employee must have prior authorization from their direct superior.

3.4. USE OF INFORMATION

Notwithstanding the other obligations established in this Policy, the following obligations must be adhered to when accessing and using the information of BH Compliance (or its Clients):

A) Users must ensure the security of the information they handle, in accordance with its classification, the requirements that safeguard the principles of confidentiality, integrity, and availability of the information, and the requirements set forth by applicable legislation, especially in matters of information security and personal data protection.

B) Users must protect information assets from unauthorized access and processing, and in general, from any occurrence of an information security incident.

C) Users must participate in information security talks and training sessions as indicated by the Responsible Party or BH Compliance.

D) Users must respect the intellectual and industrial property of BH Compliance and its Clients.

E) Users must report security incidents to the Responsible Party in accordance with section 3.5. of this Policy, and in accordance with the Security Incident Management and Reporting Policy.

Upon termination of the employment or contractual relationship with BH Compliance, as the case may be, or at any time during the course of this relationship as required, and prior to signing the respective termination agreement in the case of employees, Users must cease using all company information assets and return those in their possession, with the prohibition of taking or using information from BH Compliance (or its Clients). BH Compliance may, at any time, remove access and revoke any permissions granted."

3.5. MANAGEMENT OF INFORMATION SECURITY INCIDENTS

Security incidents (whether their occurrence or suspicion of occurrence) must be reported and managed in accordance with the Information Security Incident Management and Reporting Policy.

In addition to security incidents that may occur within BH Compliance, attention must also be given to those information security incidents that may affect BH Compliance's suppliers or any other third parties working for BH Compliance.

For example, an information security incident includes any disclosure or sending of information to unauthorized third parties, regardless of whether such disclosure is intentional or accidental; any logical access by third parties, known or unknown, to information; the loss of physical (paper) or electronic documents; theft, damage, or loss of office equipment, such as laptops and cell phones; or suspicious or unauthorized access to our offices that may jeopardize the security of information assets.

Furthermore, in implementation of the obligations of Law No. 20.393 on Criminal Liability of Legal Entities, along with Law No. 21.459 on Cybercrime, it will be considered a security incident if an event occurs that, while not necessarily meeting the requirements of the previous paragraphs, involves an attack from BH Compliance's systems to any external system, which has the potential to be classified as a cybercrime.

4. LOGICAL SECURITY MEASURES

Unauthorized third-party access to our systems can jeopardize the information of BH Compliance and its Clients. Therefore, access to BH Compliance’s computer systems will be controlled, among other measures, as follows:

A) Every employee will have a personal user account with a unique identifier and password, which will serve as a credential to uniquely identify them to access and use BH Compliance’s corporate network resources. These credentials will be personal, confidential, and non-transferable. Consequently, only the employee may use their credentials and will be responsible for any misuse of their account by unauthorized third parties resulting from their lack of care. If shared usage is required, authorization must be requested from the Responsible Party.

B) To access computers and remote desktops, the employee must enter their credentials, as specified in section A) above, and then approve access through a two-factor authentication tool.

C) Passwords must follow the guidelines established by BH Compliance, including any policies and procedures issued for this purpose.

D) All employees must use their institutional email for work-related purposes exclusively, and it is prohibited to use it for personal matters. The institutional email must be used carefully, with special attention to the information sent and the recipients. In this regard, it is prohibited to use the institutional email to subscribe to non-work-related services, social networks, make online purchases, or file personal complaints, among others.

E) Internet access using BH Compliance systems and devices must be within the limits set by applicable regulations, the Internal Regulations of Norms, Policies, and Procedures, the Employment Contract, and in any case, in an appropriate manner for the workplace.

F) Any document prepared for a client or arising from services provided to them must be registered and stored in its corresponding folder (on OneDrive or the system currently used by the company). This will allow for auditing and data recovery if necessary.

G) Penetration tests (pentests) will be conducted every 12 months, or immediately after any significant changes to our information systems. These tests will be carried out by certified information security professionals, with the goal of identifying and addressing any vulnerabilities in our digital defenses."

5. PHYSICAL SECURITY MEASURES

Unauthorized third-party access to our facilities can jeopardize the information of BH Compliance and its Clients. Therefore, physical access to BH Compliance offices will be controlled by the following measures:

A) Employees and certain third parties must use a code or password to access BH Compliance offices.

B) Meetings held physically at the offices must be coordinated in advance through the formal communication channels provided by BH Compliance. Authorized third parties (visitors) must register at the building's reception and will then be received by the Executive Assistant.

C) Employees are responsible for the authorized third parties (visitors) in the offices, so they must ensure that these individuals do not access offices or areas where they should not be.

D) Employees must immediately report suspicious activities or individuals, incidents, and the loss of their access card by sending an email to the Responsible Party at ramon.montero@bh-compliance.com."

6. USE AND SAFEGUARDING OF COMPANY DEVICES

Notwithstanding the obligations established in other sections of this Policy, Users must comply with the following obligations and prohibitions regarding the safeguarding and protection of the equipment, resources, and devices used to access or use BH Compliance's Information Assets, such as desktop computers, laptops, tablets, phones, or cell phones, regardless of ownership of these (the 'Devices').

6.1. General rules regarding the use of Devices

A) Users should not have an expectation of absolute privacy when using the Devices in any manner.

B) BH Compliance may, in accordance with applicable legislation, its internal policies, and the Internal Regulations of Order, Hygiene, and Safety, monitor the use of the Devices to ensure compliance with its policies."

6.2. Obligations regarding the use of Devices

A) Users must exercise the utmost care to protect the Equipment. In this regard, Users must physically safeguard the Devices, as well as the information contained in them.

B) Users must take all necessary measures to prevent unauthorized third-party access to the information of BH Compliance and its Clients.

C) Users must use the Devices exclusively for activities related to the performance of their duties— in the case of employees— or services necessary to provide their services— in the case of suppliers and contractors. Exceptionally, the Devices may be used for personal purposes, provided that this use (i) does not interfere with the performance of their work or service; (ii) does not otherwise affect the interests of BH Compliance, especially the security of the information; and (iii) does not involve the storage of personal information. Personal use of the Devices as described will be the sole responsibility of the User in charge of the device. The exceptional personal use described will not affect BH Compliance's authority to access, delete, or modify the information contained in a device if it aligns with its policies.

D) When using the Devices, Users must comply with all instructions or recommendations provided by BH Compliance to preserve the security and proper functioning of the Information Assets.

E) Users must keep their workstations and computer screens clear to prevent unauthorized access, loss, or damage to information.

In this regard, Users:

i. Should not leave physical documents like papers on their desk or the location where they are working or providing services, as the case may be. They should also avoid leaving password information, access codes, or similar data visible. If they leave their workstation or place of service and cannot store them, they should turn them over so they are not visible to others. ii. When leaving their desk or the place where they are working or providing services, they must store all information and lock or turn off their computer.

F) In case of loss of any Device, Users must immediately report it by sending an email to the Responsible Party.

G) Users are responsible for backing up critical information stored on the Devices.

H) At any time upon request by BH Compliance, or upon termination of the employment or contractual relationship with the company, Users must return all Devices in their possession to BH Compliance, facilitating and not obstructing access to its content.

During pandemic periods, employees must adhere to the commitments made in the Teleworking Annex incorporated into their contract.

The rules set out in sections a), b), d), and g) will apply to employee-owned equipment that has been exceptionally authorized by BH Compliance for work-related purposes.

6.3. Prohibitions regarding the use of Devices

A) It is prohibited to disable access control mechanisms, antivirus software, or any other security components of the Devices assigned by BH Compliance.

B) It is prohibited to download or install software on the Devices assigned by BH Compliance. If it is necessary to install software required for the performance of their duties, users must contact the Responsible Party at ramon.montero@bh-compliance.com.

C) It is prohibited to use the Devices assigned by BH Compliance to engage in any of the activities outlined in the following section 7. General prohibitions on use.

The rules set forth in sections a) and c) will also apply to employee-owned Devices that have been exceptionally authorized by BH Compliance for work-related purposes.

7. General prohibitions on use

Users are prohibited from using the Devices and, in general, the Information Assets of BH Compliance to:

A) Distribute defamatory, discriminatory, sexist, racist, abusive, obscene, or otherwise inappropriate messages.

B) Engage in activities that invade or may invade the privacy of a third party.

C) Engage in activities that could negatively alter the work environment or create a hostile environment.

D) Engage in activities that are illegal under applicable legislation.

E) Engage in activities that could cause embarrassment, reputational loss, or other similar harm to BH Compliance or a third party.

F) Make fraudulent offers of services or products.

G) Bypass any security system and authentication system.

H) Perform any of the following actions: port scanning, security scanning, network tracing, keylogging, unauthorized access attempts, or other information gathering techniques when they are not part of the User's duties according to their role or the services they provide to the Company.

7. INTELLECTUAL PROPERTY

7.1. General Rule

Any access to information and material from other companies or individuals must respect their intellectual property rights, and it may not be copied, modified, or forwarded without the prior written authorization of the owner of such rights.

7.2. Software

Downloading/ installing pirated or unlicensed software on the devices of or provided by BH Compliance creates a cybersecurity risk and legal liability for BH Compliance. Therefore, under no circumstances may Users download/install this type of software.

8. COMPLIANCE

All Users must comply with this Policy, as well as the rules, procedures, and any documents that may be issued for this purpose.

An information security incident may, in certain cases, constitute a crime punishable under Law No. 21.459, which establishes criminal offenses related to computer science. Unauthorized access to personal data (understood as any information related to an identified or identifiable natural person) constitutes a violation of Law No. 19.628 on the Protection of Private Life, which obligates individuals working with Personal Data to maintain confidentiality.

Users are required to report to the Responsible Party any non-compliance with the obligations derived from this Policy that they become aware of, who will take into account the particularity of each situation and adopt the appropriate and relevant measures.

Any violation of this Policy, and of the procedures or rules derived from it, by a BH Compliance employee, may result in disciplinary measures against the violator in accordance with the provisions of the BH Compliance Internal Rules of Conduct, Policies, and Procedures ("RINPP").

In accordance with the provisions of the RINPP and employment contracts, BH Compliance may monitor and analyze the use of information systems, including examining the use of BH Compliance's information and communication technologies, which are considered relevant to evaluate compliance with the Policy.

9. VALIDITY

The provisions of this Policy will come into effect six months from its approval.

10. CONTINUOUS MONITORING

As an integral part of our Information Security Policy, BH Compliance is committed to ensuring the integrity, confidentiality, and availability of all critical data. To achieve this, we implement a continuous monitoring program, which includes regular penetration testing of our applications, networks, and internet-connected devices. These tests are carried out by specialized teams on a quarterly basis. Their goal is to proactively identify and mitigate potential vulnerabilities before they can be exploited.

11. REVIEW AND CONTROL

The compliance with this Policy shall be evaluated and supervised periodically. This supervision will be the responsibility of the person in charge or whoever they delegate it to. The main result of these

evaluations will be communicated to the person in charge at the email address ramon.montero@bh-compliance.com.

The Policy will be reviewed and updated annually by the person in charge to ensure its adequacy in response to relevant changes in legislation, organizational structure, technology, or contractual obligations acquired by BH Compliance that may influence it, thus allowing for continuous and periodic improvement.

12. INQUIRIES

The Policy can be found on the intranet, in the "BH Internal Policies" folder, and will also be distributed to all BH Compliance employees.

In case of any doubts, suspicions, or verification of non-compliance with this Policy, it should be reported to the Person in Charge as soon as possible, who will provide the necessary assistance to handle the matter appropriately.