IT Policy

1 BACKGROUND AND OBJECTIVES

The Company's IT Policy applies to all employees at RiskPoint Group (the "Company") on a global basis. This policy applies to any use of the Company's IT systems, including the use of desktops and laptops, as well as mobile equipment, whether in the workplace, at home or elsewhere.

The IT Policy aims at regulating the overall principles for the employees' use of the Company's IT systems, including internet access and use of emails.

The purpose of this policy is to ensure that employees use the IT systems of the Company with care, that the Company's information is available to employees, and that employees keep such information confidential.

The Company's IT systems shall be used so that they do not:

- affect the availability of the Company's IT systems
- affect the confidentiality regarding the Company's information
- cause nuisance to the Company's employees, collaborators, customers or other parties affiliated with the Company
- damage the Company's reputation

2 PASSWORD PROTECTION

Certain parts of the Company's IT systems are subject to access control rules. The rules on access control are security measures that must be observed by all employees. Access control to the protected parts of the IT systems is carried out using a password system. Persons authorized by the Company to access the protected parts of the IT systems may receive a special password from the Company's IT Administrator.

An employee's password is personal and may not be written down or disclosed, except to the Company's IT Administrator. If a third party is suspected of having an employee's password, the employee must immediately change their password or contact the Company's IT administrator.

The employee must not change existing passwords. However, the employee is entitled to change (but not remove) their personal password. The latter must be done at least every three months, and the Company's IT systems will notify when the time is approaching.

The employee's personal password must be at least 12 characters. It must not contain the employee's initials, parts of the employee's full name, or any national special characters (e.g.: æ, ø, å, ä, ö, ï, ÿ, â, ã, ñ, ß) but must contain 1 character from each of the following 4 categories:

- uppercase letters (A-Z)
- lowercase letters (a-z)
- baseline (0-9)
- non-alphabetical characters (e.g. !, §, #,%)]

3 STORAGE OF DATA

All data, including any kind of customer material, shall be stored on the Company's servers, unless otherwise specifically agreed with the Company's IT Administrator.

4 INTERNET ACCESS AND USE OF EMAIL

The Company makes internet access and use of emails available to the employee to performance their duties of the Company. Be aware that use of the internet and emails leave an electronic track, and the Company can trace its use back to the individual employee.

All employees are assigned an email account that is established for commercial use. In the absence of an employee, a colleague may be granted access to the employee's email account. This must be approved by the Company's IT administrator and the applicable Manager.

5 VIRUSES

Virus is today one of the biggest threats to IT equipment and data. The Company's IT systems are protected by a virus scanner, but the risk will always be present. It is therefore important that all employees demonstrate common sense and do not open files from individuals or companies that are unknown to them.

The internet is the largest source of virus distribution, but since virus is also spread through physical media, it is important that these are handled with caution.

When viruses are detected in the Company's IT systems, it is recorded centrally. The registration contains information about the virus, the PC, and the employee.

6 ETHICAL STANDARDS

Internet, when used via the employee's PC or mobile phone, may be used in ways that do not violate common ethical standards.

7 THIRD PARTY RIGHTS

Files, including music files, video files and software subject to third party copyrights, may not be downloaded in violation of such rights or otherwise copied, installed or placed on the employee's PC or parts of the Company's IT systems. Similarly, such material may not be sent via email in violation of third party copyrights.

8 IT SECURITY

The internet access and use of emails must always be in accordance with this policy.

In order to ensure compliance with this policy as well as to prevent or correct system failure, the Company's IT Administrator may open any email and any attached files.

To ensure the Company's IT security, no form of private usb storage devices may be connected to the Company's IT systems.

The employee's laptop is the Company's property and may only be used by the Company's employees.

Employee's use of other IT equipment made available by the Company, including laptop, mobile phone, iPad and other similar equipment, may be used for limited private purposes in accordance with this policy. Mobile phones may not be used for premium rate services, donation of gifts to fundraising etc.

Internet access and use of emails for non-work related purposes may only be done to the extent that it is compatible with the employee's performance of the Company's duties and in accordance with this policy. Use for non-work related purposes should be limited as much as possible.

The employee is allowed to read private emails via the internet. However, the employee may not open emails from unknown persons or use links that the employee do not trust.

Additionally, our internet lines uses a MPLS protocol for routing of data, which is monitored by the provider.

9 OWNERSHIP FOR PROGRAMS, EMAILS, ETC.

Programs located on the employee's PC are considered Company property.

In connection with the termination of an employment relationship, the employee is not be entitled to copy or delete any files, programs, etc., located on the Company's servers.

Any email sent to and from the employee's email account shall be regarded as Company property.

10 TERMINATION OF EMPLOYEMENT

Termination of the employment relationship will for the sake of this section mean the time when the employee is released from performing duties for the Company.

It is the employee's responsibility that private emails are deleted from the employee's email account in connection with the termination of the employment relationship.

The Company decides when the employee's email account must be closed. The Company takes care to activate an "out-of-office message" that is automatically sent to senders of emails to the employee's email account.

Emails received after termination of employment and prior to the closing of the employee's email account will be opened by the Company.

After closing the employee's email account, all emails sent to the employee's email account will be forwarded to a Company email address where all emails are opened.

11 CONTROL

The employee's traffic on the internet is recorded in a central log file, while another central log file contains a copy of all the emails sent to and from the employee's email account.

The Company thus has the opportunity at all times to check that the employee complies with the IT policy. The Company's IT Administrator can open any email and any attached files and gain insight into any traffic on the internet.

If an employee becomes ill or is otherwise non-scheduled absent for a long period of time, the Company's IT Administrator may activate the employee's "out-of-office assistant" and also assist in accessing the email inbox if necessary for the Company's operation. The employee will be informed about this and any access will take due account of the employee's privacy.

12 INSTALLATION AND DOWNLOADING OF PROGRAMS

The employee must not install any software on the Company's servers. It is permitted for the employee to install applications on their mobile devices, as long as such applications are in compliance with this policy. If an employee wishes to install special software on the Company's server, the employee must contact the Company's IT Administrator, who, if the installation is allowed, will assist the employee.

However, it is allowed to install software necessary for the function of a printer in the employee's home.

13 USE OF SOCIAL MEDIA

Social Media means forums such as Facebook, X (formerly known as Twitter) and LinkedIn ("Social Media").

During working hours, the employee must only use Social Media to a limited extent and in any event only to such extent that does not affect the employee's performance of the duties of the Company.

Some Social Media provide associations with other users as "friends" / "connections". The employee is allowed to have the Company's customers, suppliers and other business associates as "friends" / "connections".

In the employee's communication with the Company's customers, suppliers and other business associates through Social Media, the employee must at all times comply with this policy.

If the employee is subject to a non-solicitation clause, the employee is responsible for ensuring that an update of the employee's Social Media profile in connection with a job change does not constitute a violation of the clause. In addition, the employee should be aware that actions on

Social Media can still fall under regulations covering trade secrets, including after the termination of an employment relationship.

14 GUIDELINES FOR USE OF SOCIAL MEDIA

Regardless of whether Social Media is used during or outside of working hours, the employee is obliged to comply with the guidelines found in this policy.

The employee has freedom of expression in the use of Social Media but should be aware of any local legislation such as those pertaining to slander, defamation, personal data, and similar.

Using Social Media, it is possible to share information with friends, acquaintances and business associates, and the content of Social Media can be publicly available. For this reason, the employee must always pay due attention to what information is published in these forums.

It is permitted to identify as an employee of the Company if the employee represents the Company in a loyal and professional manner. If the employee identifies themself as an employee of the Company or otherwise disclose their employment with the Company, the employee must make sure that the employee's statements should in no way be perceived as the Company's opinions. It is not allowed to present positions on behalf of the Company without prior approval.

In addition, the employee should act in manner befitting the position the employee holds at the Company.

If the employee takes pictures on the Company's premises or in Company-related contexts, e.g. of colleagues in connection with social events, the employee is not entitled to use these images on Social Media unless the photographed persons have given explicit permission.

As an employee of the Company, the employee is subject to confidentiality. This also applies to the use of Social Media, and the employee must not, for example, pass on business secrets, internal information about turnover, customer information or other confidential information via Social Media.

As an employee of the Company, the employee is subject to the general duty of loyalty. In relation to the use of Social Media, this means that the employee must refrain from speaking ill of colleagues, managers, the Company's customers, products or the like.

15 OTHER SAFETY PRECAUTIONS

The PC must always be turned off when the employee leaves the workplace at the end of work. The employee may not lend their PC to anyone or allow any unauthorized third party to use it.

16 LAPTOP PROCUREMENT AND USAGE

All laptops acquired for or on behalf of the Company are deemed to be company property. Any laptop provided must be returned at the end of employment. All purchases of Devices, must be approved or handled by IT.

Each employee provided with a laptop by the Company is responsible for the physical security of the laptop. This is regardless of whether the laptop is used in the office, at one's place of residence, or in any other location such as a hotel, conference room or while travelling.

All employees must take the following actions to ensure the physical security of Company laptops:

- When not in use, the laptop must be locked with a password and caution should be used when entering any Company passwords on the laptop.
- Laptop must not be left in a vehicle. If it is necessary to leave the laptop in a vehicle, the laptop must be locked in the trunk of the vehicle.
- When using the laptop in public areas, it must not be left unattended.
- It must not be left in checked-in luggage.

- It must be stored in a hotel room safe or locked suitcase when left alone.

If the laptop is lost or stolen, the IT department must be notified immediately.

Files stored on the physical laptop, i.e. not stored on the hosted servers, are not backed up in any way, and will be deleted occasionally. Company data must not be saved locally outside the session, unless the IT department has approved. It is the employees responsibility to ensure backup or move the data to the hosted session/server.

There is no support offered for the local usage of the laptop, and in case of need, the local data will be wiped out as part of the support action.

Support within the session follow the regular procedure by contacting Support IT's helpdesk as 1st level either by phone/email.

17 INFRINGEMENT OF THE IT POLICY

Failure to comply with the IT Policy may have employment-related consequences.

18 AUDIT OF THE IT POLICY

This policy is reviewed periodically to ensure the best possible use of the Company's IT systems, including internet access and use of emails. The changed IT Policy will come into effect once the employee has been made aware of the changes.

Version: 4
Dated: February 5, 2025