CODE.

Code of conduct

relating to security and information management

HARDIS GROUP

Summary

Introduction and purpose 5

1. Compliance with laws and regulations 5

2. General security provisions 5

2.1. Human ressources-related securit5

2.2. Security and access control

2.3. Asset management

3. Cybersecurity pratices 6

3.1. Protection against malware

3.2. Backup and business continuity

3.3. Development and maintenance

3.4. Incident and vulnerability management

3.5. Relationships with third parties

4. Use of Hardis Group ressources 8

4.1. General rules on the use of IT System resources

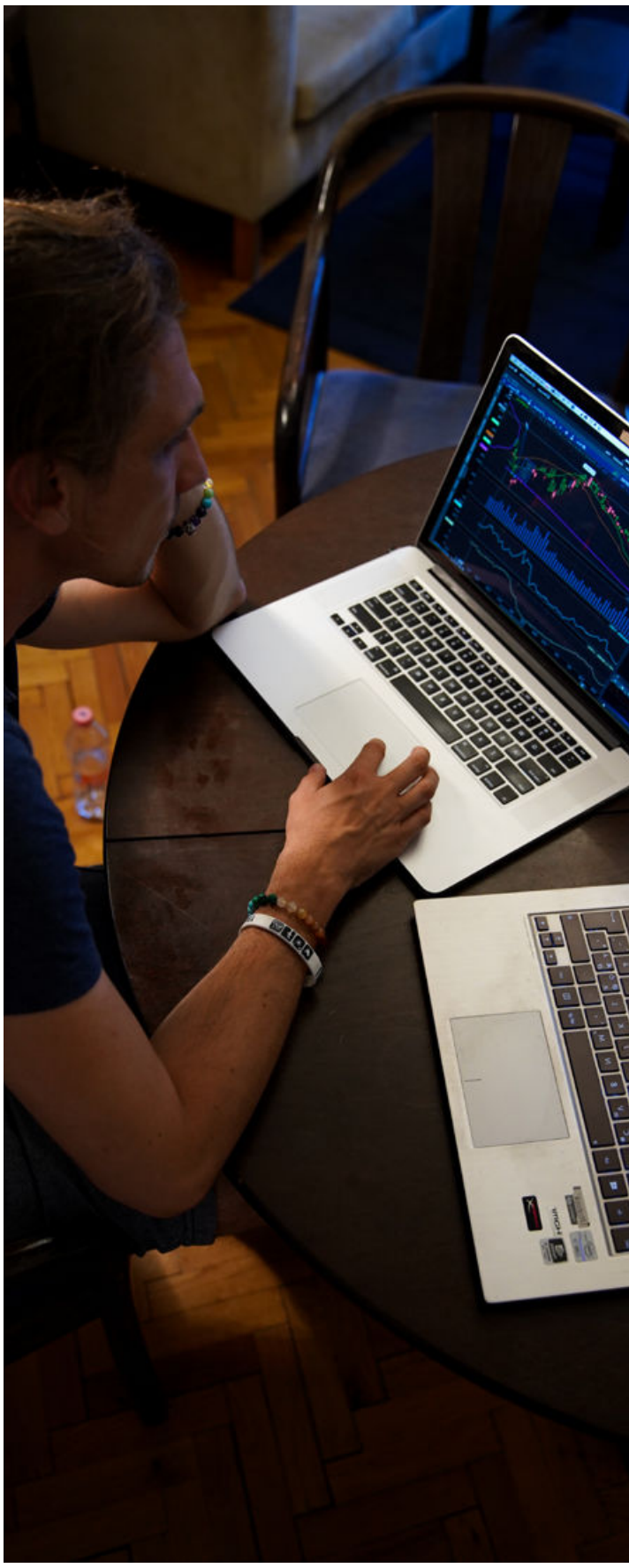
4.2. Internet use

4.3. E-mail

4.4. Storage spaces and et protection of connexion

5. Penalties for breaching this code 9

Introduction and purpose



This code of conduct (the “Code”) sets out the rules and requirements on security, information management and the use of Hardis Group and its subsidiaries resources.

The generic term “Hardis Group” refers to Hardis Group and its subsidiaries.

This Code applies to any person or entity performing services for Hardis Group, as well as to their personnel and subcontractors, if any.

This Code supplements the obligations arising from the contract(s) signed with your company. Its sets out your specific rights and duties in this area, in order to ensure that you comply with Hardis Group’s security policy when carrying out the services entrusted to you (the “Activities”).

01

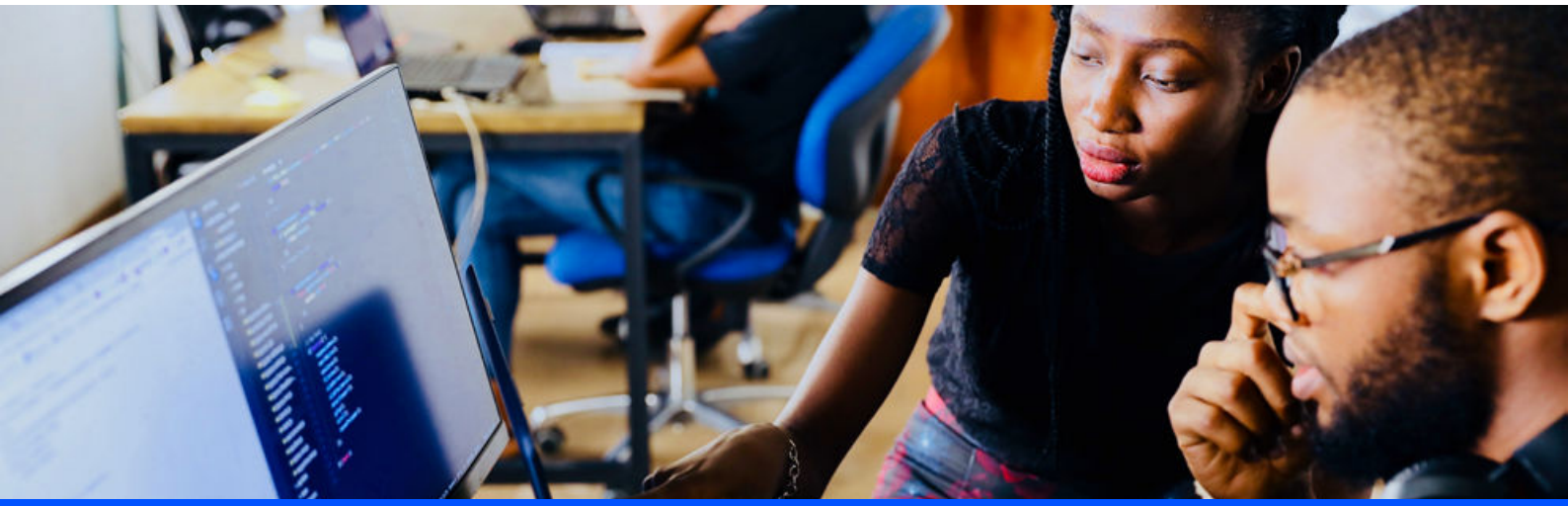
Compliance with laws and regulations

Throughout the relationship, you declare that you are and will remain compliant with all laws and regulations, and in particular with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (the "GDPR"), and that you will impose identical obligations on your personnel and on any third parties under your control (including your affiliates, agents and subcontractors, if any). Unless stated otherwise, you will ensure that Hardis Group's data is located in France, or at the very least in the European Union.

Failure to comply with these provisions may result in the immediate termination of the contract(s) between Hardis Group and your company.

Hardis Group also reserves the right to carry out an annual audit covering the scope of the Activities entrusted to you, subject to a notice period of 1 month. You will assist and cooperate fully with Hardis Group during the audit.

You will fulfil your duty to advise Hardis Group, to protect the information you receive, and never to use this information to gain any advantage.



02

General security provisions

2.1. Human ressources-related security

You will manage the identity and movements (departures, arrivals, mobility, etc.) of your personnel and any third parties under your control, individually and separately, and manage the assignment of permissions in accordance with the role and duties of the person in question and the principle of least privilege.

You will also have your personnel sign a specific confidentiality agreement if they carry out administrator duties (privileged permissions) or process sensitive or highly personal data as defined by the reglementation. This principle also applies to third parties under your control (subcontractors, agents, etc.).

You will ensure that you have a sufficient number of appropriately skilled employees in place, including by providing relevant training and awareness.

As part of these obligations, and where permitted by law, you agree to comply with information requests and criminal record checks for any personnel processing sensitive or confidential data for Hardis Group.

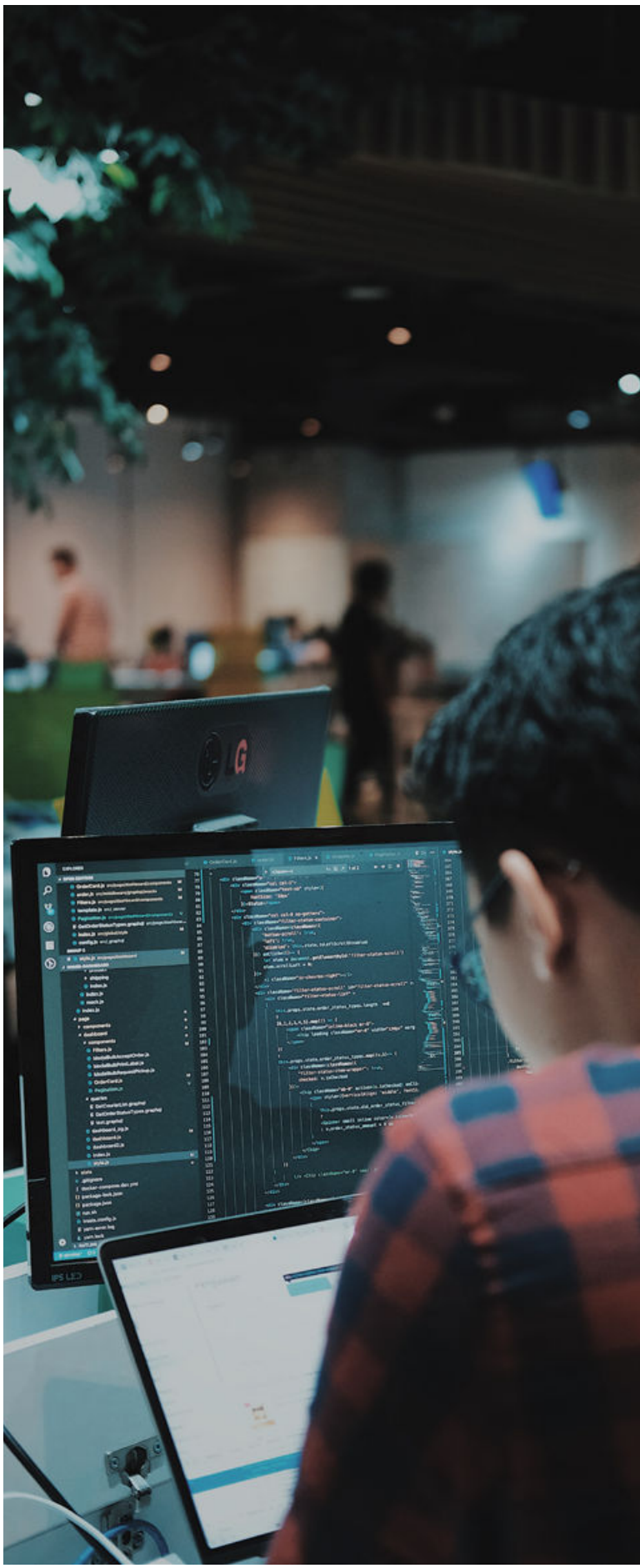
2.2. Security and access control

You will implement access controls and identify, individually and by name, each person who has access to the data and applications relating to the Activities entrusted to your company by Hardis Group. In particular, you will ensure that your premises are protected against unauthorised access. You will apply whatever security measures are necessary to protect equipment, communications and premises in accordance with applicable best practice.

2.3. Asset management

You will manage the assets connected to the Activities entrusted to your company in accordance with Hardis Group's stated needs in terms of the availability, integrity, confidentiality and traceability of processed information.

You will also return Hardis Group's assets (tangible and intangible assets, including confidential information or personal data) upon completion of the service, delete all data entrusted to you, and formally notify Hardis Group of such deletion.



03

Cybersecurity pratices

3.1. Protection against malware

You will have anti-virus and anti-malware software installed across your IT assets, and ensure that the database is up to date.

You will also have maintenance contracts in place for your IT assets, as well as the means to keep such assets secure and in good working order.

You will apply patches to all hardware and software for which you are responsible, as recommended by your providers.

Wherever necessary, you will use encryption technologies that comply with the recommendations of the French National Cybersecurity Agency (ANSSI).

3.2. Backup and business continuity

In connection with Activities entrusted to your company, you will take all necessary backup and restoration measures in order to protect the stored data.

In particular, you will retain Hardis Group's data solely for the purposes of the Activities entrusted to you and will not to use it for any other purpose. You will retain the data in accordance with best practice and with applicable laws and regulations.

You will also ensure that backups remain available at all times and are protected against integrity and confidentiality breaches. You will carry out backup restore tests, on a regular basis or at Hardis Group's request, and report on the results of such tests.

You must have a business continuity plan in place that allows you meet the agreed service level for the Activities entrusted to you.

3.3. Development and maintenance

For activities including application development work, you will apply and check the proper application of suitable guidelines and frameworks for the technology in question, consider GDPR security requirements at each stage of the software or solution life cycle, and obtain Hardis Group's written consent before making any changes to an object in production (documented and approved rollback process).

You will monitor security patch releases by software vendors within the scope of the Activities entrusted to you, and you will systematically apply a configuration and change management process, taking account of GDPR security requirements for all production launches.

3.4. Incident and vulnerability management

You have a duty to report any situation that could cause a security incident to Hardis Group.

Therefore, within the scope of the Activities entrusted to you, you will have systems and processes in place for detecting incidents, analysing reported information, qualifying situations, developing an action plan and keeping a log of users' actions that could have a security impact, such that you are ready to respond immediately when an event that could compromise system security is detected.

You will apply patches to the systems at a frequency appropriate to the criticality level of the assets, keep accessible services to a minimum, apply a policy of deleting non-essential elements (unnecessary services, accounts, etc.) and adhere to a password policy that meets the ANSSI recommendations.

You will also apply a crisis management plan within the scope of the Activities entrusted to you (stating the parties involved, a qualification procedure, a report management and crisis recovery procedure, details of resources available/used in the event of a crisis, etc.).

3.5. Relationships with third parties

You may not co-contract/subcontract the Activities entrusted to your company without the prior consent of Hardis Group.

Where a co-contracting or subcontracting arrangement is used, you will ensure that your co-contractors or subcontractors comply with the requirements set out in this Code.

04

Use of Hardis Group ressources

4.1. General rules on the use of IT System resources

You may have access to Hardis Group's IT system (the "Resources") while carrying out the Activities entrusted to your company.

All tools and Resources made available to you remain the property of Hardis Group or its licensors.

For security reasons, access to such Resources is granted on a temporary basis and may be revoked at any time at the sole discretion of Hardis Group. Any and all equipment provided to you under this arrangement must be returned without delay in the event that Hardis Group revokes access to the Resources, or where the Activities entrusted to you are terminated for whatever reason, or where the nature of your duties changes and you no longer require use of the Resources to perform the new service.

You must only access and use those Resources made available to you, or authorised for your use, by Hardis Group.

You must not breach Hardis Group's confidentiality rules or act in a way that could place Har-dis Group in a compromising situation.

Each of your employees involved in carrying out the Activities will be issued with individual credentials to access the Resources. Under no circumstances may these credentials be shared with another individual or legal entity. You therefore agree to apply best-practice rules on cre-dential storage and management.

It is your responsibility to report any and all unusual incidents or events that you may witness in the context of the Activities to: **security.alert@hardis-group.com**.

4.2. Internet use

When accessing Hardis Group Resources, you are solely responsible for the manner in which you use the internet, and in particular for the websites you visit, which must be related to the Activities. You must not disrupt the proper functioning of the Resources by making inappropriate or excessive use of the Internet, such as by breaching copyright, downloading unauthorised, illegal or inappropriate software or files, downloading large files for personal use, viewing and streaming files containing non-business-related content, etc.

You must only visit websites that are directly related to your professional activity and are useful for the performance of the duties or tasks entrusted to you.

Occasional internet use for personal reasons is tolerated within reasonable limits, provided that you do not visit websites containing content that is inappropriate or unlawful, or that could harm the reputation of Hardis Group.

4.3. E-mail

Sending and receiving emails is an essential party of day-to-day activities. Since emails may contain various types of information (some more confidential than others), you must follow the recommendations set out below for security purposes.

You will be solely responsible for the content of the messages you send or forward, and to whom you send or forward them. You must take care not to use email improperly or inappropriately in a way that could disrupt the normal functioning of the systems, such as by saving an excessive number of messages, sending messages to multiple recipients, sending unnecessary attachments, sending excessively large attachments or files without compressing them, or sharing confidential information through insecure channels.

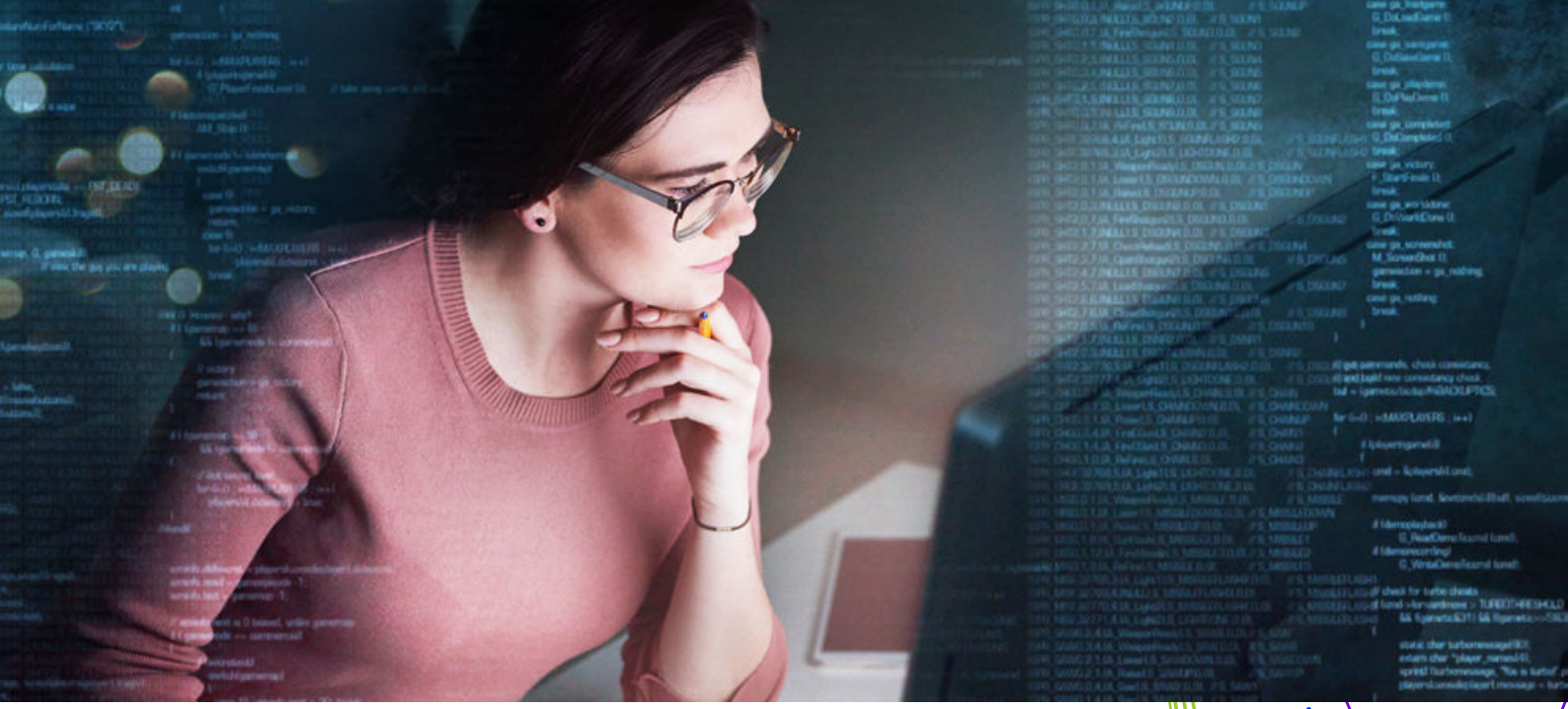
You must think carefully before opening unsolicited emails and attachments, which could amount to “phishing” attacks or contain malware.

4.4. Storage spaces and protection of connexion

Storage spaces must be secure in line with Hardis Group’s confidentiality and data protection policy. The peripheral devices made available to you by Hardis Group have been approved by Hardis Group’s IT team. You must notify this team before using any other fixed or mobile peripheral devices in the context of the Activities.

Access to IS elements, workstation sessions, applications, email and telecommunications systems, and other information system elements is protected using credentials (usernames and passwords) for which it is essential to respect the conservation rules as well as than the Hardis Group recommendations regarding password management.

You are responsible for the manner in which you use Hardis Group’s Resources. You must therefore take appropriate steps, at your level, to keep these Resources secure, and must not deliberately compromise their integrity or the normal functioning of the network.



05

Penalties for breaching this code

If you breach the rules sets out in this Code, your right to access the Resources (if any) will be suspended or restricted, without prejudice to Hardis Group's right to exercise early termination of any contract with your company relating to the

Activities on the grounds of such breach. In addition, Hardis Group or any authorised third party may pursue civil or criminal action against you.

This Code contains a set of fundamental rules that you must follow. Note that these rules are not exhaustive, and apply without prejudice to your requirement to comply with applicable laws and regulations.