Assessio Group
Banérgatan 16
Box 55673
102 15 Stockholm Sweden

ASSESSIO GROUP

Information Security Policy

Version:	2.0
Approved by:	Johan Masironi, CEO
Classification:	External

1. About this policy document

1.1 Purpose, scope, and users

This top-level policy document is aimed at defining the purpose, direction, principles, and basic information security rules.

This Policy applies to the scope of the Information Security Management System (ISMS), as provided for in ISMS document of ASSESSIO GROUP and its subsidiaries Assessio Sweden, Assessio Norway, Assessio Psychometrics, Assessio Netherlands.

1.2 Validity and document management

This document is valid from the final release date as stated in this policy document.

The owner of this document is the management of the organization. It must assess the document at least once a year and update it if necessary.

1.3 Assessio Group Executive statement

Focus and scope of the activities

The management of Assessio Group states that it has integrated a management system within the total business organisation. This management system at least complies with the applicable laws and regulations, customer requirements and wishes of the key stakeholders as well as the continuous improvement requirements that the ISO 27001;2017 imposes on the management systems.

Assessio Group

Assessio Group is a leading, innovative player in the fields of Talent Assessment, Talent Development, Talent Performance and Talent Analytics. Assessio Group is known for its innovations in the HR field. As an organization we continuously use the latest scientific insights to be able to map knowledge about the qualities of people and groups more and more extensively with valid and innovative tools. Our clients work in various industries and carry out assessments across the world with Assessio Group.

Scope

This policy refers to Assessio Group, which refers to Assessio Sweden, Assessio Norway, Assessio Psychometrics and HFMtalentindex. Because these organizations jointly provide various products and services as well as the systems they use, this policy applies to all organizations that fall within the Assessio Group. The policy is aimed at the Assessio Group's own employees, but regarding security, the Information Security Policy is also imposed on third parties. Third parties can include chain partners and cooperation partners with whom information processes are shared or information is exchanged.

Scope Assessio Group: Information security related to the development, management and delivery of online assessment tools, data analytics and providing support, training, and consultancy in the use of online assessment tools, data analytics and the resulting data in accordance with the Statement of Applicability version 3.0 dated 15th of December.

Scopes per entity:
Scope Assessio Sweden: Information security related to the delivery of online assessment tools and providing support, training, and consultancy at the use of the online assessment tools and the results it produces accordance with the Statement of Applicability version 3.0 dated 15th of December.

Scope Assessio Psychometrics: Information security related to the development of online assessment tools in accordance with the Statement of Applicability version 3.0 dated 15th of December.
Scope Assessio Norway: Information security related to the delivery of online assessment tools and providing support, training, and consultancy at the use of the online assessment tools and the resulting data in accordance with the Statement of Applicability version 3.0 dated 15th of December.

Scope HFMtalentindex: Information security related to the development, management and delivery of online assessment tools and providing support, training, and consultancy in the use of online assessment tools, data analytics and the resulting data in accordance with the Statement of Applicability version 3.0 dated 15th of December.

Risk-taking

When describing the organisation and making the business process transparent, it has been assessed whether sufficient management measures and resources (training/equipment/infrastructure) are available to manage the risks arising from the risk analyses. Where the measures were not sufficient, additional measures were taken. During the periodic reviews, the system will be assessed as if the system is still adequate, and any changes are indicated. Actions that follow from this are assigned to those responsible and systematically followed up via action lists.

Customer wishes

Within our business process, the customer's desire is central and therefore customer satisfaction is key. This ensures that our continuity is guaranteed. The wording of the customer's wishes has been achieved through the analysis of the customer contacts. These wishes have been translated into the products and services that Assessio Group provides. The management system describes how our organization ensures that we continue to comply. Each year, the experience and insight gained regarding customer and other relevant stakeholders' wishes will be updated in a consultation prior to the assessment of the management system.

Management system

The management system of Assessio Group contains the description of our processes, where the ISO 27001 standard is taken as a starting point. This executive statement is the overarching document. This document is used as a guide for the underlying document set of information security. It includes:

- Information Security Policy
- 10 golden security rules

Furthermore, the policy has been translated into various relevant procedures and attachments that are included in the management system on the Assessio Intranet on SharePoint.

Responsibilities

The management is responsible for the correct compliance of the system and to ensure that it complies with the laws and regulations. The Security Officer is responsible for managing the management system and ensures that managers have understood the goals of the management system and are able to implement the necessary regulations.

Management will assess the implementation and operation of the system (such as procedures and working regulations) according to a fixed schedule. Operational management is responsible for the operationalisation of information security policies within the operating company and departments. They shall ensure that the tasks and responsibilities are respected. Every quarter, the information security team, from which Management is a part, consults on the current information security issues within the organization.

All employees are instructed to comply with what is required by the policy and information Security Policy. In addition, tasks and responsibility are invested in the job profiles.

Awareness and training

Assessio periodically organizes various awareness sessions and training courses in the context of information security.

Information Security Policy

Ensuring the accessibility and reliability of information is an essential part of responsible business operations. Information security is the collective name for the processes, which are set up to protect the reliability of processes, the information systems used, and the data stored therein against the intentional or unintentional disaster. The term 'information security' refers to:

- availability: ensuring that information and information are available to users at the right time and place.
- confidentiality: protecting information from knowledge and mutation by unauthorized persons. Information is only accessible to those who are authorized to do so.
- integrity: ensuring the correctness, completeness, timeliness and accountability of information and information processing.

Information security aims to prevent or minimize the occurrence of threats that may impact on the above aspects of the information (systems). Threats can be of a different nature, including technical vulnerabilities, human threats ((un)intentional misconduct by users, administrators, guests, or external personnel), force majeure (lightning strike, flooding, earthquake) and technical nature (failure of communication connection, failure in technical facilities and failure in the information systems).

All employees are instructed to handle these three aspects carefully. So, with all information, make sure that it is honest, available, and where necessary confidential.

Special attention is requested for the careful handling of information, and accessibility of information. Our information classification overview explains in detail which treatment level has been determined for which information flow and system.

Information security objectives

Assessio has set itself the goal of guaranteeing and protecting the confidentiality, availability, and integrity of information. In addition, we have set ourselves the goal of preventing security incidents. To make the policy on information security concrete, processes are set up and continuously improved. At the same time, the processes and agreements in the management system are the objectives for the organisation regarding information security. The performance of the system, and therefore the objectives of the organisation, are assessed and followed up by means of the annual management assessment.

Accessibility based on need to know

For all information and information processing facilities within the organization, it is only made available if there is a need for the person concerned to obtain access.

Make necessary resources available

When describing the organisation and making the business process transparent, it was assessed whether sufficient resources (training/ equipment/ infrastructure) in the field of quality and information security are available. During the periodic review, changes are indicated and the need to make additional resources available is determined.

Corrective, preventive, and improving measures

Every employee within the organization has the right and the task to indicate points for improvement in quality and information security aspects within the organization. This with the aim: continuous improvement of the processes, structurally managing risks regarding information security and responding adequately to information incidents and deviations. An overview of the adopted control measures for the information security management system is included in the declaration of applicability.

Objectives

Annual objectives are formulated and evaluated during the annual assessment of the management system. These are drawn up per aspect, with the associated measuring points. These annual targets, together with the stakeholder risk analysis, form a living and driving part of this policy statement.

21st of December 2022

Johan Masironi
Chief Executive Officer

2. General rules on information and information handling

2.1 Ownership of information

Any data created, stored, transmitted, or received through information systems, including several applications, email, internet, fax, etc., whether it is personal or not, should be considered as the property of the organization. The exception to this is the data that the organization processes as a SaaS supplier for clients. This data is not owned by the organization but should be dealt with in line with the agreed Processor Agreements.

2.2 Clean desk & Clear screen

Within ASSESSIO GROUP, we are dealing with confidential information from our customers. This means that we must deal with this in a confidential way. To minimize the risk of unauthorized access to this data, the following rules apply.

2.2.1 Clear desk policy

1. If the authorized person is not in his/her workplace, all papers and data storage media must be labeled as sensitive (internal or confidential), from the agency or other places (printers, copiers, etc.).
2. Such documents should be stored securely to prevent unauthorized access.

2.2.2 Clear screen policy

1. No one leaves their computer (desktop/laptop/tablet/phone) "unlocked". Every time the workplace is abandoned, the device must be locked.
2. If the authorized person is not in his/her workplace, all sensitive information should be removed from the screen, and access to all screens to all systems for which the person has authorization should be denied.
3. In case of a short absence (up to 30 minutes), the clear screen policy is implemented by logging out of all systems or locking the screen with a password. If the user is away from the system for more than 30 minutes, the clear screen policy is implemented by logging out of all systems and shutting down the workstation or logging out of the workstation if the workstation goes to sleep-mode.

2.2.3 Printers, copiers, and physical mail

1. Documents containing sensitive information (internal or confidential) must be retrieved directly from the printers, and copiers.
2. Collection places for received or physical mail still to be sent must be protected by access control. Confidential mail may only be opened by the addressed person or department.
3. All paper containing sensitive or confidential information may not be disposed in a regular waste bin. Shred or use the container for sensitive documents which can be sealed.

2.3 Exchange of information

1. Confidential data and business-sensitive information may not be sent or transferred to third parties without the consent of the management.
2. Confidential (telephone) calls should not be made in public places, and if privacy of persons involved or sensitivity of information plays a role, the conversations should not take place in the shared office environment but in a dedicated room.
3. Voicemails and text messages (SMS/WhatsApp) should not contain confidential information.
4. Posting confidential data and business-sensitive information on removable media is not permitted.
5. It is not allowed to exchange information through removable media. (USB sticks, portable hard drives)..
6. It is not allowed to store confidential business information on remote network or Internet locations other than on shared sources such as the fileserver and managed secure (private) cloud storage (SharePoint, Teams). The exchange of company information by e-mail is only permitted through the e-mail account made available in the domains of ASSESSIO GROUP.
7. Sharing confidential information must take place through shared resources such as the server.

2.4 Treatment of information

1. Interchangeable media such as external hard drives, USB sticks, DVDs and CDs should not be used for permanent storage, for example as backup, without the permission of the information owner and Security Officer.
2. Confidential information is not transferred to physical (portable) media if possible. If this is necessary because other transfers are not possible or desirable, then when transferring physical media with information (disks, USB sticks, etc.) to external parties, the receiving party should be required to provide a signed statement indicating at what time, at what location and to which person the transfer took place. The receipt must also include a description of the type of information medium and the information contained on the physical media.
3. Company documents must always be at the location available by the organization is saved so that these documents go along with the backup and remain available to the organization.
4. Documents to be edited offline on a laptop should be stored on the personal network disk.
5. It is not permitted to delete relevant data for ASSESSIO GROUP without permission.
6. Do not leave confidential data and business-sensitive information unattended on a printer or display.

2.5 Transport of confidential information

When you bring confidential information from the office, you are responsible for the security of this information. Think of documents that have customer data on it, or usernames and passwords.

3 Policy for acceptable use of assets

3.1 What are Assets?

1. This policy means all the means provided by the organization for creating, modifying, communicating, sharing and destroying business information, for example corporate network (LAN, Wi-Fi), business applications, workstations, laptop computers, mobile and landline phones, printers, etc.

3.2 General terms of use ICT resources

1. Employees are personally responsible for the ICT resources they have on loan and they must ensure that those funds remain available.
2. Employees should ensure that updates or patches and other system settings (can) be performed, and that the equipment is equipped with up-to-date virus protection.
3. Outside working hours, it is necessary to log out. When leaving the workplace, the workstation must be locked. If, under special circumstances, outside working hours is required, it should also be logged out when the work is terminated.
4. Set a mobile device such as a mobile phone or tablet so that it is automatically locked with password or PIN if it is not used for up to 30 seconds.
5. Portable equipment containing important, sensitive, or critical information should not be left unattended and, if possible, it should be physically locked up, or special locks should be used to secure the equipment.
6. Portable equipment should be transported in a proper (laptop) bag.
7. Do not leave portable devices such as a laptop or a mobile phone, left in unattended spaces, such as cars, meeting rooms, or public spaces.
8. When portable computer equipment is used in public spaces, the user should ensure that the data cannot be read by an unauthorized person.
9. Users are responsible for storing information in the appropriate shared sources, even if they are outside the (organization's) site. This related to the management of information and making backups.
10. Portable equipment should in principle only be used for business purposes.
11. Private use of ICT resources is limited. Use for ancillary activities is always prohibited unless written consent has been obtained separately.

3.3 Receipt and return of ICT resources

1. Upon receipt of ICT resources, the employee must sign up for receipt and compliance with the user regulations under the loan agreement.
2. At the end of employment or hiring period, the employee must return the ICT resources taken on loan to the system administrator. Faulty equipment must also be returned. The employee receives proof on request that the ICT resources have been handed in and reports this to HR so that the 'checklist can be updated from service.
3. In the case of change to another department, employees must return the ICT resources taken on loan to the system administrator, unless it is agreed that the ICT resources will also mutate to the future department.
4. Before the ICT resources are handed in, employees should ensure that all company-relevant digital data present here is secured for future use.

3.4 Taking assets off-site

1. Information labeled with qualification HIGH on one of the categories of the Confidentiality, Integrity, Availability classification and/or which, in the case of disclosure to third parties, may damage the organization's image or competitiveness and/or bear the Company Confidential label, may not be taken outside the office building (digital or on paper) without the express consent (express consent may also consist of the available to the employee of a connection infrastructure such as VPN) outside the office building (digital or on paper), or on systems outside the office building (by sending, storing, uploading, etc.).

3.5 Unmanaged assets

1. Users should:
   1.1. end active sessions when they're done.
   1.2. log out of the device when the session ends.
   1.3. laptops, tablets, and other mobile devices using a lock or similar security (password).

3.6 Antivirus protection on assets

1. To prevent possible malware infection as much as possible, ASSESSIO GROUP has installed a virus scanner.
2. The antivirus software used by the organization must be activated on any computer with automatic updates.

3.7 Use software and applications

1. Business use of downloaded or proprietary software and applications is only permitted if they are legal and cannot harm ASSESSIO GROUP's systems.
2. Private use of downloaded or proprietary software and applications is not allowed.
3. Downloaded or personal software and applications must be scanned for viruses and malware before they are used and installed by the system administrator or by the employee with the express permission of the system administrator.
4. The use of software that performs a specific function independently without or with little user intervention is only permitted on condition that it is strictly necessary for the specific function.
5. It is not permitted to download large amounts of data from the business systems and ASSESSIO GROUP software products and services used or to systematically copy substantial portions of files or databases of the company systems used and ASSESSIO GROUP software products and services.

3.8 Email usage

1. Employees are prohibited from using other email systems or storage servers, such as Google, Dropbox, or WeTransfer for company-related activities, unlike the systems and servers offered by ASSESSIO GROUP.
2. The e-mail system is intended for business traffic. Employees are entitled to make limited use of the e- mail system for receiving and sending personal e-mail messages, if this is not disruptive to the day-to-day work and business. Non-ASSESSIO GROUP-related business use is always prohibited.
3. When sending confidential and classified information, encryption (encryption) of the message will be used.
4. Leaving personal information or email addresses on the Internet should be handled with restraint as this can become a source of spam mail.
5. The employee's right to receive and send personal e-mail messages is bound by the following conditions:

5.1. The email will contain the sender's name and a disclaimer.

5.2. The employee is not allowed to log in under a different name and read another person's email messages and files, unless the holder of the email address has explicitly consented to it.

5.3. Falsifying or manipulating email messages is prohibited. For example, when forwarding e-mail, the address, sender or email itself changes the content without the recipient being able to know.

5.4. It is not permitted to send threatening, sexually harassing or sexually explicit messages, pornographic material, or racist messages.

5.5. It is not permitted to send messages that conflict with ASSESSIO GROUP's business interests.

5.6. It is not permitted to download and/or send copyright protected software.

5.7. It is not permitted to send e-mail messages which the sender should reasonably suspect to be regarded as inappropriate by the employer or are not desired by the recipient.

6. It is strictly prohibited to use of Company email to:

6.1. Send messages anonymously or under a fictitious name.

6.2. Send or forward messages threatening, abusive, sexual, racist or discriminatory messages and chain mail.

6.3. Harass someone through digital channels.

7. The employer will not read the content of personal e-mail messages if they are identifiable as such. Also, the associated personal information is not registered and/or verified. However, where there is a serious suspicion of fraud or a situation in which the organization can be seriously harmed, the employer may check the employee's e-mail on an incidental basis. In such a case, the employer is always obliged to inform the employee afterwards, even if nothing irregular has been detected during the check. Before initiating a check, the employer will always consult current (privacy) laws, regardless of whether the employee is legally allowed to check.

3.9 Internet

1. The Internet system is intended for business purposes. Employees are entitled to make limited use of the Internet system for private purposes, if this is not disruptive to the day-to-day work, the proper day-to- day operations and the costs associated with this use are kept to a minimum.

2. It is prohibited use of the organization’s Internet (connection):

2.1. To visit sites containing pornographic, racist, discriminatory, offensive, or offensive material.

2.2. View or download pornographic, racist, discriminatory, offensive or offensive material.

2.3. Visit private sites that need to be paid for.

2.4. To provide unauthorized access to non-public sources on the Internet.

2.5. Deliberately change or destroy information over the Internet to which access has been obtained without permission.

2.6. Filesharing or Streaming Services (such as Internet radio, Netflix, or Spotify) when it generates excessive data traffic, such that it may compromise the availability of the facilities.

2.7. generate incoming private messages by participating in chat programs, non-business newsgroups, subscriptions to e-magazines, newsletters, and the like. In any case, unacceptable private use means playing and/or downloading games, shopping, gambling and/or participating in gambling and visiting chat-chat programs.

3. In principle, the employer will not record and/or monitor personal data about internet use, such as time usage and sites visited. This is without prejudice to the fact that controls on an occasional basis may take place for a serious reason (e.g., in case of suspected unacceptable use).

4. The user should consider all information received through unverified websites to be unreliable. Such information can be used for business purposes only after its authenticity and accuracy has been verified.

5. Downloading software and applications for business use is only permitted provided that written permission has been granted in advance by the management. This consent is granted only if the applicable rights are met and any licenses are paid. Downloading files and internet sites should be limited to highly necessary use, including in relation to the risks of bringing in viruses.

6. Downloading software and applications for private use is not allowed. If viruses are obtained by private downloading files and internet sites, the employee is fully liable for the damage caused by them. This also applies if this damage has occurred to the client of ASSESSIO GROUP, where the employee carries out work.
7. Unintentional security breaches, inside or outside the organization, must be reported directly to the security officer and/or management.
8. The user is responsible for all possible consequences arising from the unauthorized or inappropriate use of internet services or content (content).
9. It is also otherwise not permitted to act on the Internet in violation of the law or in an unethical manner.
10. Management may block access to certain internet pages for individual users, user groups, or all employees of the organization. If access to some web pages is blocked, the user may submit a written request to management for authorization to access such pages. The user should not use a detour. The user should not attempt to circumvent this restriction independently.

3.10 Use of social media

1. ASSESSIO GROUP supports the open dialogue and exchange of ideas and sharing the employee's knowledge with peers and third parties through social media (such as LinkedIn, YouTube, or Twitter). In the case of related topics, the employee should ensure that the profile and content are in line with how he would present himself in text, image, and sound in front of colleagues, customers, and suppliers.
2. Directors, managers, executives, and others who promote policies or strategy on behalf of ASSESSIO GROUP have a particular responsibility when using social media, even if the content is not directly related to their work. Based on their position, they must check whether they can publish in a personal capacity. They are aware that employees, customers, and suppliers read what they write.
3. This also applies if employees participate in social media from private computers or internet connections, but only insofar as participation can affect the work.
4. When employee sets up a social media account that is directly work related, it should be always registered in THE Name of ASSESSIO GROUP. Upon termination of employment, the employee and employer will find an appropriate solution for the transfer of the management of this profile or the information and contacts thereto.
5. All expressions on social media should follow the guidelines as set out by the marketing and communication department of ASSESSIO GROUP.

3.11 Phone calls

1. The telephone system, including any mobile phone made available, is intended for business traffic. Employees are entitled to make limited use of the telephone system for making personal telephone calls, if this is not disruptive to the day-to-day work and the good business.
2. In principle, the use of information numbers such as commercial pay numbers, as well as international telephone traffic by the employee to make personal telephone calls is not permitted
3. It is not permitted to have threatening, sexually harassing or sexually harassed conversations or racist conversations.
4. It is not permitted to hold conversations that conflict with ASSESSIO GROUP's business interests.
5. ASSESSIO GROUP will not read the telephone numbers of personal calls, if they are identifiable as such, in principle. Personal data will also not be registered and/or verified. This is without prejudice to the fact that checks on an occasional basis may take place because of a serious reason, in the opinion of the employer.

4 Encryption policy

1. Information which leaves the internal organization’s network and is classified as HIGH on confidentiality and/or HIGH on integrity is encrypted and sent over a secure connection only.
2. Encryption takes place in accordance with “best practices”, where required encryption becomes stronger as data becomes more sensitive.
3. If employees work on private equipment, ASSESSIO GROUP is authorized to enforce security settings on this equipment (e.g., hard drive encryption or installation of security software).
4. Confidential and secret information is shared through the secure environment made available for this purpose, not through services such as social networks and cloud services (Dropbox, Gmail, etc.).
5. There is a secure storage location that can only include system management and IT Management, where security certificates and "private keys" are stored.
6. All keys will be replaced before the expiry of validity. If a key has not been granted validity, a validity of one year is applied.
7. Applied keys are never deleted but archived within the "vault" to decrypt any data encrypted with an old key in case necessary.
8. Keys for data are stored in accordance with the retention period for the data itself, to always be able to decrypt data in case necessary.
9. Application for new keys is made on behalf of or formal approval of the IT Manager.
10. Store business information on mobile devices should only be provided if encryption is present on the mobile device.

5 Remote Working Policy

1. The organization requires all employees to use business information and customer data during remote working with the same security measures as are applied when working in the office.
2. The organization permits use of only authorized hardware and software even while working from home.
3. The equipment, tools and supplies provided by the Assessio Group must be used only by authorized person for business purpose only. Also, it is employee’s duty to care of Assessio Group’s belongings and contact the immediate manager in case there is an issue.
4. Remote working is only made available for relevant functions after the approval of the management.
5. Remote working is only allowed in locations where 'free' work can be done, i.e., no people or cameras can have a view of the input (keyboard) and display (screen).
6. It is not allowed to use public networks. When you need internet access, always use a secure connection.
7. No company information may be transferred to non-ASSESSIO GROUP equipment or to a third-party network.
8. Storage on portable equipment should be synchronized with the company network at least once a week.
9. When leaving the PC, the PC must be locked using a password.
10. Passwords should not be stored automatically (including in the browser) without the need for an additional authentication factor (fingerprint recognition, MFA).
11. All employees must take care of their own physical and mental health, stay safe during working remotely and maintain work-life balance.
12. The manager and employee must agree on the communication channel that would be used to be in touch (e.g., Teams, Slack etc.).

6 User accounts and password policies

1. Preferably, use a password manager to generate your password.

2. Personal accounts are connected to one person, meaning that login information may not be shared, not even with colleagues
3. Passwords should not be written down on paper or saved in a file. If it is necessary, make sure it is stored safely (e.g., not on a memo on your desk).
4. If the security of a password is in doubt– for example, if it appears that an unauthorized person has logged in to the account — the password must be changed immediately, and the security officer must be informed.
5. Default passwords — such as those created for new employees when they start or those that protect new systems when they're initially set up — must be changed as quickly as possible.
6. Stay away from using numbers that mean something to you (phone numbers, social security numbers, street addresses etc.).
7. Employees may never share their passwords with any outside parties, including those claiming to be representatives of a business partner with a legitimate need to access a system.
8. Employees may only share their passwords with colleagues after explicit approval by management or the security officer.
9. Employees should take steps to avoid phishing scams and other attempts by hackers to steal passwords and other sensitive information.
10. Passwords may not be stored or saved in browsers or other password tools / vaults other than those approved of by Assessio management.
11. If you need access to specific systems or portals, your supervisor or the security officer will provide access for you.
12. When a user account is terminated or blocked (i.e., at the end of an employment term or contract period) the employee must ensure that all relevant company data will be transferred to the account of the supervisor. Access to this account can only be granted in extremely exceptional circumstances and with explicit permission of management.

7 Privacy and data processing

7.1 Privacy

1. Data that can be traced back to a person will not be recorded, collected, verified, combined, or edited, unlike agreed in this Protocol.
2. Personal information will only be used for the purpose for which they were collected.
3. The registration of data that can be traced back to a person is kept to a minimum. The aim is to respect the privacy of employees in the workplace.

7.2 Computing

1. The General Data Processing Regulation (GDPR) put demands on the storage and processing of personal data and the requirements for carrying out appropriate technical and organizational measures to protect personal data from loss and unlawful processing.
2. The processing of most personal data is necessary to execute our employment contract. In addition, some data is subject to a legal obligation (e.g., the Payroll Tax Act). The organization does not provide (copies of) identity documents of employees to third parties (e.g., to leasing companies).

7.3 Copyright / Intellectual property rights

1. Users should not make unauthorized copies of software owned by the organization, except in cases where it is permitted by law, by the owner or the manager.

2. Users are not allowed to copy software or other original material from other sources and are liable for any consequences that may arise under intellectual property laws of organization-related tasks.
3. Copyright is the sole right of the creator of a work of literature, science, or art, or of its right-holders, to make it public and to multiply it, subject to the restrictions, set by law. Employees may not infringe third- party copyright.

8 The rights and obligations of employees

8.1 Employees' rights

1. Perusal law: employees have the right to view the data registered about him or her.
2. Copy right: employees have the right to receive a copy of the dates registered on him or her.
3. Correction right: employees have the right to (have) corrected or supplemented incorrect data from the registered data.
4. Right of removal: employees have the right to (have) the data registered about him or her, which are no longer relevant, or contrary to the organization's information security policy, or to (have) a legal requirement removed and destroyed.

8.2 Reporting obligation

1. If it is found that the above-mentioned rules of conduct are violated by one or more persons, this should be reported to the Management Board.
2. If an employee has improperly used resources or authorization (even if they were granted in a previous role), this should be notified to management immediately.
3. All technical incidents involving IT facilities must be reported to the system administrator. An incident with a major impact must be reported directly to the management. High-impact incidents include incidents that relate to the availability of multiple users or the integrity or confidentiality of a large amount of information.
4. Weaknesses that threaten the availability, integrity or confidentiality of information should be reported immediately to the management. It is not allowed to abuse or exploit these vulnerabilities, even to show that there is a shortcoming.

8.3 Reporting data breaches and information security incidents

1. If there is a (suspicion of a) data breach or information security incident, this should be reported to the security officer without any delay.
2. In the case of a data breach, it involves access to or destruction, modification, or release of personal data to an organization without the intention of this organization.
   2.1. Examples of data breaches are a lost USB stick with personal data, a stolen laptop/tablet/phone or an intrusion into a data file by a hacker.
3. In the event of an information security incident, there is a breach of Availability, Integrity and/or Confidentiality of information.
   3.1. Examples of information security incidents include unauthorized access to information, use of illegal or expired licenses, virus, or malware infection, missing or theft of equipment or media that contain data.
4. The security officer assesses data breaches based on the guidelines to report whether a report is made to the data authority and any data involved.

8.4 Reporting vulnerabilities

1. Any employee, vendor, or third party who comes into contact with the organization's data and/or systems should report any vulnerability, incident, or event as a (possible) incident.

9 Control

1. Samples or security tests may be carried out to ensure the safety of the network and to ensure careful use in accordance with this scheme. In addition, the technical integrity and availability of the infrastructure and services is monitored. The monitoring of use will consist of random monitoring of the use of the Internet (time use, sites visited). To this end, anonymous lists of visited internet sites can be requested and analyzed. E-mail traffic can also be analyzed randomly by intercepting emails, anonymizing and reporting the internal employee.
2. Incoming Internet and email traffic are monitored as well as possible for viruses, spam mail and similar discomfort. If it turns out that an email contains a virus (or a file with a particular extension) that cannot be deleted, it will be automatically stopped, and the sender and recipient are informed. If, nevertheless, an e-mail that may contain a virus is received, the recipient should contact the system administrator without delay
3. If it turns out that this scheme is being violated or if there are indications (such as complaints, signals from inside or outside the organization and system failures), the data of the employee(s) concerned may be turned on, viewed, and used. Checking internet and e-mail use and calling behavior as well as opening e-mail for the purpose of detecting unlawful conduct by the employee is therefore permitted if there is a reasonable suspicion or suspicion of unlawful conduct. This also applies to private use.
4. The relevant data shall be retained if this is necessary for an employee as part of further investigation and any action to be taken, complying with the legally permitted retention period. Of course, this information is handled very carefully.

10 Disciplinary process

1. In the case of action in accordance with these regulations or the generally applicable legal rules, the management may take disciplinary action depending on the nature and seriousness of the infringement. This includes a warning, reprimand, transfer, suspension, and termination of the employment contract. In addition, the Management Board may decide whether to temporarily restrict access to certain ICT facilities.
2. In the case of a suspicion of criminal conduct, the organization may report it to the authorities.
3. An investigation into alleged abuse to be launched is recorded in writing. In a conversation with the manager and the HR manager, the employee is confronted with the findings and given the opportunity to give his/her views on what happened.
4. Disciplinary measures (except a warning) cannot be taken solely based on a processing of personal data carried out by automated processes, such as the finding of an automatic filter or blockade via, for example, an antivirus package. Furthermore, no disciplinary action shall be taken without the employee having been given the opportunity to express his views.
5. In addition, it is possible that ASSESSIO GROUP will introduce a temporary blockade of the facility in question in the event of an (automated) observation of nuisance. This blockade will be maintained until the cause has been removed. If the cause is repeated, disciplinary action may be taken.

11 Reservation

Failure to comply with these regulations may lead to human measures by the Management Board. All cases where this Regulation does not provide for an assessment of the management.