ISMS 04 Acceptable Use Policy

new cognito

Document control

Date	Version	Change by	Job title	Description of change
15.10.2024	0	Alon Chokler	Security Expert	Create basic document outline
15.10.2024	1	Shai Ohana	CISO	Document review
01.09.2025	1	Ronen Ben Shlush	CISO	Document review

Document approval

Date	Version	Approved by	Job title
01.09.2025	1	Sérgio Lopes	CEO

Table of content

1. General

Effective security is a team effort involving the participation and support of every employee and affiliate related to the company who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. Goal

The purpose of this policy is to outline the acceptable use of computer equipment at the Company. These rules are in place to protect the employee and Company. Inappropriate use exposes the Company to risks including virus attacks, compromise of network systems and services, and legal issues.

3. Definition

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Company business or interact with internal networks and business systems, whether owned or leased by Company, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Company and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Company policies and standards, and local laws and regulation.

This policy applies to employees, contractors, consultants, temporaries, and other workers at Company, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the Company.

When employees' smart phones and/or laptop/workstation are not the organization's property, the organization cannot force to set them to certain settings. However, it expects and asks its employees to set them up as requested.

4. Responsibility

CISO.

5. Operation method

Acceptable use policy

Please ensure you have read and understood the following summary of the main points of the organization’s policies regarding information security.

5.1. General

Prior to commencing your work, it is essential to acquaint yourself with the organization's security policies, procedures, and any specific instructions related to your tasks. Please be mindful that your utilization of the organization's computer and communication systems may be subject to monitoring and/or recording for legitimate purposes. Furthermore, you are required to consistently adhere to all legal, statutory, or contractual obligations that the organization deems relevant to your position. Failure to comply with this policy may result in disciplinary action, up to and including termination of employment.

5.2. Handling of assets and Sensitive Data

To ensure the utmost security of sensitive information, it is essential to adhere to the following protocols:

1. Proper Labeling: Whenever you generate classified material, it must be appropriately labeled following the guidelines provided. This ensures that it remains well-protected throughout its lifecycle.
2. Comprehensive Protection: Take utmost care in safeguarding any classified material you send, receive, store, or process, whether in electronic or physical form. Adhere strictly to the assigned level of classification to maintain its confidentiality.
3. Secure Transmission: Under no circumstances should classified information be sent over the Internet via email or other channels without implementing appropriate security measures, such as encryption. This is crucial to prevent unauthorized access.
4. Accurate Recipient Information: Always verify and enter the correct email address(es) of recipients when handling classified data to prevent any potential compromises.
5. Vigilance at Work: Exercise caution to avoid unauthorized individuals from viewing sensitive information while you are working. Take necessary precautions when printing classified material.
6. Secure Storage and Disposal: Classified printed material should be stored securely, and when it is no longer needed, it must be correctly and thoroughly destroyed to ensure it doesn't fall into the wrong hands.
7. Computer Security: Never leave your computer unattended, especially when logged in to your user account. Unauthorized access to information must be prevented at all costs, even when you are away from your workstation.

8. Informing Prior Departure: If you plan to leave the organization, it is your responsibility to inform your manager before departing about any significant information stored in your user account or in locations with restricted access.
9. Unless you have a business need, you are not allowed to download customer data. Once the need arises, the information should be deleted immediately after use.

5.3. Access Control

Your responsibility involves the use and safeguarding of the user credentials provided to you, such as user accounts, passwords, access tokens, or any other relevant items.

Here are some guidelines to adhere to:

1. Create strong passwords in accordance with organization policies and ensure that they are known only to you. Avoid sharing passwords or writing them down.
2. Avoid using the same password or similar variations for multiple user accounts to enhance security.
3. Under no circumstances should you use someone else's user account and password to access the organization's systems.
4. Refrain from using privileged user accounts, which have elevated system access, for regular business activities.
5. Access only those computer systems for which you have been explicitly granted authorized access.
6. Never attempt to bypass or undermine system security controls or use them for purposes other than their intended use.
7. Do not connect unauthorized devices to the organization's network to prevent potential security risks.

5.4. Mobile Device

Mobile devices, including laptops, notebooks, tablet devices, smartphones, and smartwatches, are essential tools for business purposes within the organization. To ensure the security and proper use of these devices, the following guidelines must be strictly adhered to:

1. Use of Organization-Provided Devices: Only mobile devices provided by the organization should be used to handle or process classified information unless explicit authorization is given.
2. Equipment and Information Handling: Equipment or information should not be removed from the organization's premises without appropriate approval.

3. Security Measures Outside Premises: When carrying mobile devices outside the organization's premises, take necessary precautions to protect them from theft or unauthorized access. For example, avoid leaving laptops unattended or visible in a car to prevent opportunistic theft.
4. Preservation of Identifying Marks: Do not remove any identifying marks, such as company asset tags or serial numbers, from the device. Store the device securely and ensure the key to access it is not easily accessible.
5. Data Encryption: Whenever possible, ensure that the device's data is encrypted and can only be accessed with the appropriate password. If the device comes with built-in encryption, do not disable it.
6. Network Connectivity: Try to avoid using public networks in crowded places such as cafes, malls, or airports. In such cases, always prefer using your smartphone's hotspot or a paid network.
7. Software Installation: The organization permits the use of leading market software such as Microsoft, Adobe, and similar. In any case of software installation, it must be used strictly according to its licensing terms, and under no circumstances should pirated or illegal software be used. If you are unsure whether a particular software is allowed, please contact the IT team for assistance with verification.

5.5. Electronic Messaging Guidelines

Electronic messaging encompasses email, SMS texts, messaging apps, web chats, and social media platforms. When using these communication channels, adhere to the following guidelines:

Official Business Communication: Utilize organization-provided electronic messaging facilities for all official business communications. Avoid using personal accounts for this purpose.

Treating Organization Messages: Consider all organization messages as official communications and handle them accordingly with professionalism and confidentiality.

Content Restrictions: Do not send messages containing defamatory, obscene, or inappropriate material, and ensure compliance with the organization's equality and diversity policy.

Prohibited Uses: Organization electronic messaging facilities must not be used for the following purposes:

1. Distributing unsolicited commercial or advertising material, chain letters, or any form of junk mail to other organizations.
2. Sending material that infringes on copyright or intellectual property rights of others.
3. Engaging in activities that corrupt, destroy, or disrupt other users' data or work.

4. Distributing offensive, obscene, or indecent images, data, or material.
5. Transmitting content that causes annoyance, inconvenience, or anxiety to others.
6. Conveying abusive, threatening, or bullying messages to others.
7. Encouraging discrimination based on race, gender, sexual orientation, marital status, disability, political or religious beliefs.
8. Sending defamatory or deceptive material.
9. Violating the privacy of other users.
10. Sending anonymous messages without clear identification of the sender.
11. Engaging in activities that may bring disrepute to the organization.

Consultation: If unsure whether a message complies with the guidelines, consult your line manager before sending it.

Phishing Awareness: Be cautious about potential phishing attempts, where malicious attachments or links to fraudulent websites are used to steal information. Report suspicious messages to the service desk without opening attachments or clicking on links.

5.6. Internet browsing

Internet access on organization-owned devices is primarily intended for work-related tasks, including accessing pertinent information, updating organization-owned websites and social media accounts, conducting electronic commerce, performing research, and other job-related responsibilities.

Personal use of the Internet is permitted, as long as it does not interfere with your duties.

However, the following activities are strictly prohibited when using Internet access:

1. Accessing Inappropriate Content: Creating, downloading, uploading, or accessing websites that contain pornography or other material considered illegal, obscene, or offensive.
2. Peer-to-Peer Networks and File Sharing: Subscribing to, entering, or using peer-to-peer networks or installing software that enables the sharing of music, video, or image files.
3. Online Betting: Subscribing to, entering, or using online betting sites.
4. "Money Making" Sites and Programs: Subscribing to or entering "money making" sites or using "money making" programs.
5. Private Business Activities: Running a private business on organization-owned devices.
6. Unauthorized Software: Downloading software that does not comply with the organization's software policy.

It is important to note that the above list provides examples of "unsuitable" usage, but it is not exhaustive. "Unsuitable" material includes data, images, audio files, or video files, the transmission of which is illegal, as well as any material contrary to the spirit and rules of this and other organizational policies.

Additionally, you must avoid websites flagged by anti-malware or browser software as potentially unsafe or suspicious.

It is your responsibility to use the Internet access provided by the organization responsibly and in alignment with these guidelines.

5.7. Cloud computing

We fully leverage the potential of cloud computing to empower our business processes with unmatched responsiveness and flexibility. Through a meticulous due diligence procedure, we carefully assess and select cloud services that align seamlessly with our specific business, security, and legal prerequisites.

It is imperative that you exclusively utilize cloud services approved and provided by the organization. We prioritize the protection and confidentiality of classified information, which is why storing such data in any unapproved cloud services is strictly prohibited.

5.8. Use of social media

At our organization, social media plays a vital role in facilitating direct communication with our valued customers. It serves as a key component of our marketing endeavors, enabling us to extend support for our products and services and gather valuable feedback to gauge public perception, to maintain a consistent and professional approach, access to corporate social media accounts and representing the organization to the general public is limited to authorized personnel and is contingent upon specific job roles.

It is essential that only approved accounts are utilized for publishing messages and responding to other users on relevant social media platforms. Using personal accounts for these purposes is strictly discouraged to ensure clear delineation between personal and corporate communications.

We recognize and respect your personal online activity as an avenue for self-expression. However, it is crucial to remember that your responsibilities to the organization extend beyond working hours. Upholding the organization's values and principles in your digital presence is paramount.

When engaging on social media topics pertinent to our organization, it is imperative to explicitly state that your expressions reflect your personal opinions and not the official stance of the organization. Transparency fosters open dialogue and reinforces the individuality of perspectives.

5.9. Privacy and compliance

In the realm of business operations, the organization carries a legal responsibility to adhere to all relevant laws that impact its activities. As employees, it is incumbent upon us to actively contribute to meeting these requirements, particularly in domains like data privacy, intellectual property, and governance.

A crucial aspect of this responsibility is adhering to the organization's policies and regulations concerning the handling of personal data. Throughout your work, it is imperative to consistently follow these guidelines, ensuring that the processing of personal data is carried out in a manner that aligns with organizational standards.

Furthermore, it is vital to be well-versed in the rules governing the use of intellectual property owned by others. Whether it pertains to software, videos, music, books, documentation, photographs, or logos, exercising caution to avoid any infringement on copyrights and other protective measures is of utmost importance.

When engaging with third parties, it becomes paramount to safeguard the intellectual property of the organization. Whether in negotiations, collaborations, or any form of interaction, ensuring the proper protection of the organization's intellectual assets should be at the forefront of our efforts.

5.10. Information security incidents

If you detect, suspect, or witness an incident that may be a security breach or if you observe any security weaknesses in our systems or services, you should first inform your line manager or contact the CISO. Unusual or unexplained events, such as messages appearing on your device, should be reported as soon as possible. If an incident is detected by us, you may be asked to take specific actions, such as logging off systems or shutting down your device. Please comply with such requests promptly.

5.11. Theft or loss of computing and communication equipment

When a company's computing equipment is stolen or lost, it is crucial to take immediate actions to ensure data security. Here are the steps that an employee should follow to safeguard the information:

1. Report the Incident: The first step is to report the theft or loss to the company's IT department or designated security personnel immediately.

Prompt reporting is essential to initiate the necessary response measures promptly.

2. Activate Remote Wiping: If the device has sensitive data and is equipped with remote wiping capabilities, IT should be notified to initiate a remote wipe. This action will erase all data on the stolen or lost device, preventing unauthorized access.
3. Change Passwords and Credentials: In the event of a stolen device, assume that login credentials might be compromised. Therefore, the employee should change passwords for all accounts that were accessible from the lost device. This includes email accounts, cloud services, and any other sensitive platforms.
4. Inform Security Personnel: The company's security team should be made aware of the incident. They can investigate the situation, assess potential risks, and implement any necessary security measures to mitigate further damage.
5. Review Access Privileges: The IT department should review and revoke any access privileges granted to the lost or stolen device. This step ensures that the thief cannot use the device as a gateway to access sensitive company information.
6. Notify Management and HR: The incident should be reported to the relevant management and Human Resources personnel. They can assess if any confidential information or sensitive data was stored on the device and take appropriate actions accordingly.
7. Assess Data Backup and Recovery: Verify if the data stored on the lost or stolen device was adequately backed up. Data recovery procedures should be implemented if necessary to restore any critical information.

6. Appendix

Nothing to add.