

Code of Conduct

DOCUMENT REFERENCE**DATE****AUTHOR****VERSION**

ISMS-COC-20260724-14

24 July 2026

Saber Ferjani (CEO)

1.4

Table of Contents

I. Requirements.....3

1 Clear desk & Clear screen3

2 Working remotely.....3

3 Visitor registration3

4 Bring your own device (BYOD)3

5 Software update3

6 Miscellaneous3

Document history

Version	Description	Reviewed and approved by/on
1.0	Initial version	Saber Ferjani / 14 October 2024
1.1	Updated section 6 with environment-related guidelines.	Saber Ferjani / 25 October 2024
1.2	Added a section for business sustainability	Saber Ferjani / 31 January 2025
1.3	Added a section for Use of AI solutions	Saber Ferjani / 11 July 2025
1.4	General update, in accordance with the RBC	Saber Ferjani / 24 July 2026

I. Requirements

1 Working remotely

- Employees shall take appropriate measures to protect the non-public information of the company and customers and partners, so that they are granted access to the company's assets for work purposes.
- Employees shall only use encrypted networks (at least WPA2) from trusted service provider to access company accounts.

2 Clear desk & Clear screen

- Computers must be locked when the desk is unoccupied.
- Laptops, tablets, and other hardware devices must be removed from the desk and locked in a drawer or filing cabinet.
- Keys for accessing drawers or filing cabinets should not be left unattended at a desk.
- All forms of documents that contain non-public information must be shredded when no longer needed.

3 Visitor registration

- When one (or multiple) visitor(s) is expected, the accompanying employee shall fill in the [visitor logbook](#).
- The reception shall be notified and asked to cross-check the visitor identity.

4 Bring your own device (BYOD)

- If the employee needs to access project information from a device that is not owned by the company, such device shall be enrolled first. Please contact the CTO/ISO for this purpose.
- Use of Signal messaging app is allowed on non-enrolled devices, if the app is protected with a PIN code.

5 Software update

- Install security updates and patches immediately upon notification.
- Automatic updates must be enabled where possible.

6 Use of AI solutions

- AI solutions can be used only with information classified as Public (See: [Information classification and retention policy \[1\]](#)).
- Provider of AI solutions shall be onboarded and reviewed regularly according [Vendor on/off-boarding process \[2\]](#).
- AI solutions shall not be integrated with environments that host customer information.
- The scope of AI-powered features that are included in Office365 is restricted to prevent potential exposure of customer data.

7 Miscellaneous

- Employees are informed about the house rules of the host (IWG / Spaces) listed here (See: [PreviewHouseRule.pdf \[3\]](#)).

- Employees are responsible for keeping the company-owned devices (including computer, access badge, and hardware security keys) safe.
- Access credentials to the company's accounts and services shall be stored using the password manager provided by the company.
- Any suspicious activity in the office premises, or company's equipment, including loss or theft of equipment, shall be reported to the CTO/ISO.
- This code of conduct as well as all ISMS policies and processes require the participation of staff to be successful.
- Anyone found to have violated one of the company policies may be subject to disciplinary action, as described in [Information security policy](#).

I. References

- [1]. Information Classification and Protection Policy, 31 January 2025, version 1.3, CYRIS360
- [2]. Vendor on/off-boarding process, 25 October 2025, version 1.1 CYRIS360
- [3]. House rules, April 2026, IWG