APPENDIX A

SECURITY POLICY:

Employee IT (Information Technology) Usage

Objective

The purpose of this policy is to protect Schindler employees, partners and the company from illegal or damaging actions related to the use of IT Resources. Inappropriate use exposes Schindler to risks including virus attacks, compromise of network system, and legal issues. Employee found to have violated this policy may be subject to disciplinary actions up to employment termination.

Everybody's Support is Needed

Effective security is a team effort. Therefore, it is the responsibility of every IT user to know, apply, and accept these guidelines.

Scope

This policy applies to all employees, contractors, consultants, and other workers at Schindler, including all personnel affiliated with third parties. This policy applies to all IT infrastructure owned or leased by Schindler.

Hardware and Software Ownership

The IT infrastructure (e.g. computer equipment, software, operating systems, storage media, network accounts) is the property of Schindler.

Data Ownership and Privacy

Data created by users on the corporate systems remain the property of Schindler. In order to protect Schindler's network, management will not guarantee the confidentiality of private information stored in Schindler's IT infrastructure. Besides, for security and maintenance purposes, authorized individuals within Schindler reserve the rights to monitor and audit equipment, systems and network traffic at any time.

Private use of IT Resources

IT users should not use Schindler's resources for private purposes. Specifically, the use of Internet services related to pornographic and illegal material, hacker tools and games is prohibited. In case of uncertainty, employees should consult their supervisor, the HR responsible or their local Information Security Officer.

Keep Confidential Information Confidential

1. Never communicate your user name and password.
2. Store highly confidential information in an encrypted form (e.g. in encrypted Lotus Notes databases).
3. Do not provide information about Schindler employees (including lists of employees) to outside parties.
4. Never provide internal business information (e.g. paper documents, e-mail documents, video or audio recordings, …) to any external individuals outside legitimate information flows.
5. Never video or audio record meetings using any device such as laptops, PDAs, audio/video recorders, teleconferencing equipment unless agreed upon by all individuals in the meeting room and approved by the meeting chairperson; in this context, it is the responsibility of the meeting chairperson to ensure that teleconferencing devices are off unless required by the meeting.

Help us Keep our IT Resources Up and Running

1. Do not change the original hardware (i.e. do not add new cables, communication systems etc.) or software of your IT resources yourself: this is the job of IT specialists.
2. Do not open attachments of e-mails (specially from unknown senders) unless you are confident that they do not contain viruses or other harmful files. In case of doubt, contact IT support before opening an attachment.
3. Do not introduce malicious programs or hacking tools.
4. Do not install anything that may bypass the firewalls protecting our Intranet.
5. Do not install or operate Wireless LAN access points connected to the Schindler network.

Abide by the Law

1. Do not violate any copyrights, trade secrets, patents or other intellectual properties. Never install "pirated" (unlicensed) software or and do not copy and/or distribute copyrighted material (software, photographs, movies, music, etc). The Employee that violates this rule will be held legally responsible.
2. Do not send unsolicited mass e-mail messages (spam). Do not modify the e-mail header information.
3. Do not intend to access data you are no entitled to access.

Date: 26-4-2023 Employee Signature: