UK Product Security and Telecommunications Infrastructure Statement Of Compliance

We, RISCO Ltd., as manufacturer, hereby declare, that the below products covered in this document are in conformance with the applicable security requirements in Schedule 1 of The Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023.

Manufacturer's Name	RISCO Ltd.
Manufacturer's Address	14 Hachoma Street, Rishon LeZion,Israel
Primary contact name:	Mark Taylor
Primary contact email address:	mark.taylor@Riscogroup.com
Product Type/Brand	LightSYS Plus,LightSYS Air, RisControl,Video Door Bell,RISCO Cloud, VUpoint Cameras and NVR
Model	RP432MP, RP432MPNW,RW332Mx,RP432KPTx, RVDBA701x,RVNVRx,RVCMx
UK Defined Support Period	5 years (Until 12/03/2029) Please note that this statement of compliance including the Defined Support Period stated herein, is only applicable to products sold in the UK.

I declare that the information contained in the table below is publicly available and undergoes regular review to ensure its continued relevance to the listed products.

Requirement	**Manufacturers documented response (URL links to documentation in the public domain)**
Passwords	RISCO is ISO 27001 and GDPR compliance ,Passwords are used for various purposes at RISCO Group. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. We are using Azure SQL as a service - the database file itself is encrypted. In the RISCO cloud each user has its own password, To protect the customer data in the RISCO Cloud, we use DB encryption for storing the data, we do not store passwords at all, we use TLS1.2 for communication, and we do not export DB information . RISCO follows the GDPR regulation and acts according to "RISCO Password Policy". Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of RISCO Group's entire corporate network. As such, all RISCO Group employees (including contractors and vendors with access to RISCO Group systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Information on how to report security issues	RISCO developed a Incident Response Plan procedure and protocol to follow in the event of a security breach, system outage, or any other incident that could potentially disrupt operations or compromise security. If customers discover a service vulnerability, they should take the following steps: 1. **Identification**: If you identify a security vulnerability or issue concerning to our services, products, or systems, kindly proceed to report them. 2. **Reporting Channel**: Please send detailed information regarding the security issue via email to @RISCO. 3. **Acknowledgment:** Upon receiving your report, RISCO will promptly acknowledge receipt and begin the investigation process. 4. **Investigation and Response**: We'll conduct a comprehensive investigation into the reported issue, prioritizing security matters, and ensure a prompt and thorough response. 5. **Resolution**: In the event of a confirmed vulnerability, RISCO will work diligently to address it promptly, safeguarding the security and integrity of our systems and services.
Information on minimum security update periods	RISCO developed a Information Security Policy and Procedures this is the top-level statement of the RISCO Group information security hierarchy. It is considered to be the basis for all RISCO Group information security regulations. This Information Security Policy defines information security as the protection of information from loss of confidentiality, integrity and/or availability. The scope of this Policy includes all information which is stored, processed, transmitted or printed using any system or storage medium. The Policy applies to all RISCO Group staff and to all other individuals who directly or indirectly use or support the services or information of RISCO Group or any of its operating entities. RISCO directly communicates product software updates to Installer/customers via Email(Technical Note), either prior to or at the time of the update.

Signed,

Motti Barad, Certification Engineer
Rishon Lezion, Israel
12/03/2024