Document ID	Revision	Date	Document category	
AAGS-HOSP-SWP-003	**1**	**2022-02-28**	**Guideline**	
Confidentiality level			Status	Page (of)
Public			**Approved**	**1 (3)**

Security Best Practices

Recommended Security Best Practices for Hospitality Products and Solutions

1. Introduction

As the global leader in access solutions, we take physical and digital security very seriously. These matters are becoming increasingly complex, but we continuously work on strengthening the security for our customers and ourselves.

In line with our policies and security best practices, we are committed to creating safe and reliable products. As part of that commitment, we are continuously assessing to improve our technology.

1.1. Purpose

This document contains guidelines and recommendations that customers can use to increase security resilience at their property.

2. Security Best Practices

2.1. General Recommendations

- Always have the latest software and firmware installed to benefit from the latest functionality updates and security enhancements.
- Make sure to use standards and cybersecurity frameworks such as NIST (National Institute of Standards and Technology) to get detailed security recommendations.
- Do not share login credentials unencrypted (e.g., via unencrypted email).
- Follow product-specific security recommendations described in the respective product manual.

2.2. Doors and Locks

- Make sure to use known secure RFID card technology (see our recommendation about RFID Credential Security Pyramid).
- Any space under the door should be covered to prevent any tools from gaining unauthorized access. If spaces under the door cannot be covered, twisting the inside door handle 90 degrees downwards will make it harder to use such tools.
- Beware of any suspicious activity, such as signs of tampering with doors or locks.
- Perform a key rotation if you ever detect an intrusion or exploit at your property and with a regular cadence for compliance with cybersecurity standards.

2.3. Network

Follow appropriate network security best practices such as:

- Restrict and segment network access to the systems and peripheral devices.
- Monitor the network for any signs of intrusions.

2.4. Authorized Service Personnel

Ensure that all service personnel are authenticated from an authorized partner.

2.5. Additional Security

Extra security such as CCTV, elevator access control, and one-way fire doors will increase general hotel security and make it harder for criminals to operate.

2.6. Hospitality Product Security Center

We provide security information and advisories for our products and services at Hospitality Product Security Center. In case of any vulnerabilities impacting our products or services, we publish advisories in accordance with our responsible disclosure policy.

3. Questions

For further questions about the solutions and security, please contact your local sales office or business partner.

4. Terms of Use