kaspersky

Approved by: [redacted]

Signature:

Publication date: 01/12/2021

Effective date: 24/11/2021

Security policy when using bionic devices

Purpose of this document

This policy governs procedures for using bionic devices in Kaspersky and aims to reduce the risks associated with these types of devices and the specific characteristics of their use in Kaspersky's business processes.

The document offers a range of standardization processes to better enhance security, while also being more inclusive of employees who use bionic devices when in the office. The policy is a public document aiming to engage the global IT and augmentation community in the discussion. As a result, we hope to pursue a collaborative effort to achieve secure use of bionic devices, such as ensuring digital privacy of data stored on devices, providing different levels of access to stored information or analyzing potential risks and threats related to human health.

Contact for further questions and ideas for cooperation: augmentedfuture@kaspersky.com.

Scope of application

This document is for use across the entire company and applies to all business units. It applies to the entire access control system, as well as administration processes, maintenance processes, and the use of automated Kaspersky systems. This policy is mandatory and applies to all Kaspersky employees and temporary staff, as well as employees of third-party companies that render contract services to Kaspersky.

Definitions

- A bionic device is one that replaces or augments part of the human body with an artificial device (implant). These include:
    - Chip implants (implanted into the body/skin)
        - An NFC biochip is a chip implanted under the skin, which uses NFC (near field communication) technology to transfer data
    - Bionic limb prostheses (arms/legs) and internal organs
    - Artificial sensory organs (visual prostheses, hearing aids)

- ACS stands for access control system.

Use of various bionic devices at Kaspersky

NFC biochips

NFC biochips are the most common bionic devices at Kaspersky. When placed next to a turnstile reader, they serve to identify employees in the access control system (replacing widely used employee ID cards). The following section of this policy covers the different security zones at Kaspersky and the procedure for using an NFC biochip to access them.

Entering a security zone

Kaspersky has four different security zones:

- Green — This is for areas adjacent to office buildings, where employees and guest vehicles can be parked or diesel generators located, as well as for loading and unloading zones
- Yellow — This includes lobbies and rooms before the turnstiles
- Blue — This area represents lobbies and rooms beyond the turnstiles, as well as underground parking facilities
- Red — This designation is for restricted areas where access is strictly limited. Access to these areas is governed by the Procedure for Accessing Restricted Areas. These areas include data centers, server rooms, storage rooms, and other sensitive places that ordinary employees should not be able to access

Green and yellow security zones can be accessed without identity verification or a pass (including a guest pass).

Blue security zones are accessed by presenting the NFC biochip to the reader on a turnstile. The ACS controller records the chip number when employees arrive at work. It indicates what access rights an employee has.

To get new access to blue zones or red zones, employees must send a request to the Service Desk. When requesting access, indicate the business reason why access should be granted. In several parts of the Kaspersky office building, the ACS also uses the following methods to confirm employee identities:

- Voice recognition
- Fingerprints

For more information on how the office is divided into security zones, please see the Regulations on Access Control and Site Security.

NFC biochip tokens are not provided for temporary or guest access.

Do NOT:

- Use your NFC biochip to allow an unauthorized person or employee to access the office

In this scenario, if an NFC biochip is used, with or without authorization, then the Information Security Department and Service Desk should be immediately notified.

Patch-management

For all bionic devices present in Kaspersky, a patch-management procedure should be carried out in compliance with the following Service Level Agreement (SLA):

- Critical updates (CVSS > 7):
    - When requested by the IS department or Product Security - the minimum possible time (no more than one week from the release of the update);
    - In a regular mode - 30 days from the date of release of the update in the vendor's update channel or from the date when the resource is installed.
- Important updates (CVSS > 5):
    - 30 days from the date of release of the update to the vendor’s update channel or from the date of resource installation.

- Non-critical updates (CVSS <= 5):
    - 90 days from the date of release of the update in the vendor's update channel or from the date of resource installation.

If updates cannot be installed (e.g. if the update causes operational problems), an exception should be agreed with the IS department and the risks caused by an out-of-date software version should be mitigated by other methods.

Dismissal of an employee

When an employee is dismissed, all of the employee's access rights must be removed from the ACS.

Requirements for NFC biochips

An NFC biochip must have the following characteristics:

1. At least 1KB of memory
2. A unique ID consisting of no less than 32 characters
3. At least two memory blocks, each having its own key and access level
4. Support for strong cryptographic encryption standards (AES, GOST 34.12-2018, etc.)

Bionic limb prostheses, artificial internal organs and artificial sensory organs

Kaspersky does not restrict the use of bionic limb protheses (arms/legs), artificial internal organs (for example, pacemakers), and artificial sensory organs (visual prostheses, hearing aids).

Metal detectors and employees with bionic prostheses

Employees who have bionic limb prostheses or artificial internal organs are exempt from the requirement to pass through metal detectors. To prove the existence of a bionic implant (for example, a pacemaker), the employee must submit a doctor's note to the security department.

Workspaces for employees with artificial sensory organs

Workspaces for employees that have artificial sensory organs require special measures. In particular, this includes preventing the potential disclosure of confidential information over audiovisual channels by appropriately separating (using a partition, for example) departments and/or employees. Partitions must be opaque and noise-cancelling.

Restrictions on certain types of bionic devices

Some bionic devices can secretly gather information (for example, by secretly recording audio or video files, or by using built-in interfaces such as GPS or Wi-Fi). These devices must be reported to the Information Security Department in advance to get approval, or the HR department must be notified during the hiring process. To determine the specifications, the model of the bionic device must be identified and indicated.

Security in locations with elevated electromagnetic radiation

Rooms with elevated electric fields (greater than 6.5 V/m) are restricted to employees with bionic implants. Employees must be informed that these rooms are restricted.

Consequences of non-compliance

Failure to fully comply with the aforementioned requirements subjects Kaspersky to the following risks:

- Theft of confidential information
- Theft of biometric and medical information
- Malicious intrusion of Kaspersky premises
- Disclosure of information not intended for publication
- Reputational harm
- Direct financial losses

Kaspersky employees who fail to fully comply with the requirements of this policy will incur disciplinary action.

Revision history

Ver.	Action (and description of changes)	Date	Responsible party	Status
1	Document development finished	24 November 2021	[redacted]	Completed

Approvers

No.	Approver	Date	Signature
1	[redacted]	24 November 2021	
2	[redacted]	24 November 2021	
3	[redacted]	24 November 2021	
4	[redacted]	24 November 2021	

www.kaspersky.com/
www.securelist.com