Security Policy

KIT-CERT

Contents

1   About this document

1.1   Abstract

This policy describes exceptions from KITs security policy to KIT-CERT in order to fulfill its duties.

1.2   Canonical location

The newest version of this document shall be located at: https://www.cert.kit.edu/p/security_policy

1.3   Version History

The current version is 1cff029. It was published on 2023-12-12.

Date	Description
2023-11-27	Add the canonical location for this document
2023-03-24	Initial publication of the Security Policy

2   Security Policy

KIT-CERT adheres in most parts to KIT's IuK-Ordnung[1], but has some additional degrees of freedom for running systems and using KITNet in order to keep the infrastructure secure.

2.1   E-Mail without malware scans

KIT-CERT may run an inbox without malware scan to receive malware samples.

2.2   Adapted spam policy

E-Mails that are routed to KIT-CERT are excluded from spam detection in order to not reject user reports on phishing, fraud or other spam.

2.3   Firewall exceptions

KIT-CERT runs systems that are able to bypass the KIT's firewall to perform vulnerability scans.

References

[1]   *Ordnung für die digitale Informationsverarbeitung und Kommunikation (IuK) am Karlsruher Institut für Technologie (KIT)*. URL: https://www.cert.kit.edu/p/iuk-ordnung.