Video Surveillance Policy

1.0 Purpose

DigiCert, Inc., and its affiliates ("DigiCert") operate video surveillance systems on DigiCert premises for the safety and security of its buildings, assets, staff, and visitors. This Video Surveillance Policy ("Policy") describes DigiCert's video surveillance practices and the safeguards that DigiCert has in place to protect the personal data, privacy, fundamental rights, and legitimate interests of those recorded on the video surveillance system.

This Policy works in tandem with the *Workforce Monitoring Policy*. This Policy also works alongside, and employees receive notice of video surveillance practices in the *Employee Privacy Notice* and of workforce monitoring in the *Global Employee Policy Guide* upon hire. DigiCert notifies all persons, including employees and non-employees, that DigiCert will process their Surveillance Data. Notice is provided prior to entering the area under surveillance.

2.0 Definitions

Video Surveillance Data ("Surveillance Data"): refers to video recordings, images, and other information about employees and visitors that are created, observed, monitored, surveilled, tracked, recorded, and otherwise documented and/or retrievable on the DigiCert video surveillance systems.

3.0 Scope

This Policy applies to:

(1) All DigiCert employees that monitor Surveillance Data through DigiCert video surveillance systems; and

(2) All cameras, devices, systems, and/or other technology that record and document Surveillance Data in connection with DigiCert video surveillance systems.

4.0 Policy

4.1 Legitimate Business Purpose

DigiCert uses, records, and retrieves Surveillance Data for legitimate business purposes only and does so in a manner consistent with applicable privacy laws, the *Workforce Monitoring Policy*, and other applicable policies. Legitimate business purposes include monitoring the safety and security of its buildings, assets, staff, and visitors, and other legitimate purposes permissible under the law.

4.1.2 Prohibitions

Installing cameras in areas where there is a reasonable expectation of privacy is prohibited. Such areas include, but are not limited to, locker rooms, bathrooms, or similar private areas.

4.2 Use of Surveillance Data

DigiCert uses, records, and retrieves Surveillance Data for legitimate business purposes only. DigiCert does not sell, transfer, or disclose Surveillance Data to third parties, except as described below.

4.2.1 Periodic Audits

DigiCert shares Surveillance Data with third-party auditors on a periodic basis.

4.2.2 Service Providers

DigiCert shares information with third-party service providers that assist DigiCert in monitoring and verifying alerts in ceremony rooms.

4.2.3 Other Exceptions

DigiCert may periodically retrieve and share Surveillance Data for other permissible purposes. For example, retrieving Surveillance Data to monitor employee misconduct and other permissible purposes under the law. Such exceptions must be approved by the DPO.

4.3 Recording & Retention

DigiCert generally records and retains Surveillance Data for up to 90 days or for as long as necessary to carry out the legitimate purposes specified under paragraph 4.1.

4.4 Data Subject Rights

You have a right to request access to Surveillance Data that includes video recordings of you and/or your images. You also have a right to request deletion (also referred to as "erasure") of such video and images, subject to the DigiCert retention practices, described above under paragraph 4.3, and subject to any overriding legitimate grounds DigiCert may have in retaining your Surveillance Data, as permitted under Article 17 of the GDPR and other applicable privacy laws. You may also object to video surveillance, subject to any compelling legitimate grounds DigiCert may have in processing your Surveillance Data, as described under paragraph 4.1, and as permitted under Article 21 of the GDPR and other applicable privacy laws.

You may exercise your privacy rights by emailing dpo@digicert.com.

5.0 Contact Details

Please contact the DigiCert Data Privacy Officer ("DPO") with any questions or concerns about this privacy notice or our data collection practices at dpo@digicert.com.

6.0 Violations

Violation of this Policy may result in discipline, up to and including termination of employment.

7.0 References

Employee Privacy Notice
Global Employee Privacy Guide
Workforce Monitoring Policy