Privacy Policy and Notice

CCTV Policy

Personal Data Protection Policy for CCTV Usage

ServerToday (Thailand) Co., Ltd.

ServerToday (Thailand) Co., Ltd. ("the Company") uses Closed-Circuit Television (CCTV) equipment to monitor areas within and around its premises to protect life and property. The Company collects personal data of customers, vendors, employees, directors, contractors, visitors, and all persons entering monitored areas (collectively "you"), both inside buildings and surrounding areas, via CCTV. This policy provides information about how the Company collects, uses, discloses, and transfers personally identifiable information ("personal data"). The Company may amend this policy at any time. Please visit this policy regularly to follow any changes. The Company will notify you of significant changes where possible.

1. Data We Collect

The Company collects still images, moving images, audio, and images of objects (e.g., your vehicles) when you enter monitored areas within buildings and premises via CCTV ("CCTV Data"). In some cases, the Company may collect, use, or disclose your sensitive personal data (e.g., facial recognition data), only with your explicit consent or as permitted by law.

2. Purposes of Collection, Use, and Disclosure

The Company may collect, use, disclose, transfer, and carry out any action including but not limited to recording, retaining, adjusting, changing, editing, destroying, deleting, recovering, combining, copying, transmitting, storing, separating, updating, or adding to CCTV data and other related personal data of yours, for the following "CCTV installation purposes":

- To protect safety, including your property
- To protect buildings, premises, and property from damage, disruption, destruction, and other crimes
- To support effective dispute resolution during disciplinary or grievance proceedings
- To support investigations or proceedings related to whistleblowing

- To support law enforcement agencies in deterring, preventing, and detecting crime, including prosecution when crime occurs
- To support the establishment of rights or defenses in civil litigation, including but not limited to labor cases
- To verify identity and to comply with applicable laws

CCTV cameras are installed in visible locations. Areas where CCTV will NOT be installed include changing rooms, restrooms, shower rooms, or other areas designated as rest areas with a high level of privacy for employees, as the Company deems appropriate.

CCTV operates 24 hours a day, every day, and may include audio recording.

Signs are installed at entry and exit points and in monitored areas to inform you that CCTV is in operation in the area.

3. Legal Basis

Legitimate Interest: It is necessary for the legitimate interests of the Company to protect the health and safety of individuals, including their property, and to protect the Company's buildings, premises, and assets, and to carry out other actions in accordance with the CCTV installation purposes. The Company will endeavor to balance its legitimate interests and the legitimate interests of relevant third parties, as the case may be, with your fundamental rights and freedoms in protecting CCTV data related to you. The Company will also endeavor to find appropriate procedures and methods to achieve such balance.

4. Data Sharing & Disclosure

The Company will keep CCTV data related to you confidential and will not disclose or transfer such data to anyone unless necessary for legitimate purposes. The Company may disclose or transfer data to carefully selected third parties, both current and future, authorized persons, and/or service providers, in accordance with the CCTV installation purposes stated in this policy.

Third parties to whom the Company may disclose CCTV data and other personal data related to you include:

- Affiliated companies: The Company may disclose or transfer CCTV data and other personal data related to you to affiliated companies for the legitimate interests of the Company and its affiliates in fulfilling the CCTV installation purposes.

- Government agencies and/or law enforcement: The Company may disclose CCTV data and other personal data related to you to comply with law, or to support or assist law enforcement agencies in investigations or proceedings in civil or criminal cases.
- External service providers: The Company may disclose or transfer CCTV data and other personal data related to you to external service providers to carry out necessary steps to protect the health, safety, and property of individuals.

5. Cross-Border Data Transfers

The Company may disclose or transfer your CCTV personal data to other countries to carry out necessary steps to protect your health, safety, and property. Such disclosure or transfer will only be made with your consent, unless there are other important legal grounds (e.g., to perform a contract between the Company and another person for your benefit) as required by applicable law.

If your CCTV personal data is transferred to a destination country with inadequate data protection standards as determined under Thai personal data protection law, the Company will take necessary steps to protect the transferred personal data to ensure it receives the same level of protection as the Company provides under the applicable personal data protection law in effect at that time.

6. Security Measures

The Company uses appropriate organizational, technical, physical, and administrative measures to protect CCTV personal data from unauthorized or unlawful destruction, loss, access, use, modification, or disclosure, aiming to maintain confidentiality, accuracy, and availability of data in accordance with minimum legal standards.

The Company has established appropriate access rights and controls for storage and processing equipment, permitting only authorized personnel with clearly defined duties and responsibilities, to prevent unauthorized access, unauthorized copying, or theft of data and equipment.

Additionally, measures are in place to record and audit access, modification, deletion, or transfer of CCTV data to enhance confidence in the appropriate control and auditing of personal data usage.

7. Data Retention Period

The Company will retain your CCTV personal data in the Company's systems for the period necessary to fulfill the CCTV installation purposes stated in this policy. When the Company is no longer legally permitted to retain your CCTV personal data, it will be deleted from the Company's systems and records. However, in cases of court or disciplinary proceedings, your CCTV personal data may be retained until such proceedings are concluded, including any possible appeal period, after which the data will be deleted or archived as required by applicable law.

8. Data Subject Rights

Data subjects have the following rights under applicable law and its exceptions:

8.1 Right to Access

- You may request access to or copies of your CCTV data. The Company will process the request within 30 days. Requests may be denied if contrary to law, court order, or if it affects others' rights.

8.2 Right to Rectification

- You may request correction of your data to ensure it is accurate, current, and not misleading.

8.3 Right to Erasure

- You may request deletion or anonymization of your data, unless the Company is legally obligated to retain it.

8.4 Right to Data Portability

- You may request to receive or have the Company transfer your personal data in an automated format to another person, where technically feasible. Service fees may apply as permitted by law.

8.5 Right to Object

- You may object to the processing of your data, except where necessary for contractual or legal obligations.

8.6 Right to Restrict Processing

- You may request that the Company restrict the use of your data in certain cases, with processing limited as required by law.

8.7 Right to Withdraw Consent

- You may withdraw consent at any time by contacting the Company through the designated channels, unless restricted by law or contract.

8.8 Right to Complain

- You may file a complaint with a government agency if the Company violates or fails to comply with personal data protection law.

9. Contact Information

If you have questions about this policy or wish to exercise your data subject rights under applicable law, please contact the Company through the following channels:

Data Controller

ServerToday (Thailand) Co., Ltd.

111/128 Moo 2, Ratchaphruek Rd., Bangraknoi, Mueang Nonthaburi, Nonthaburi 11000

Email dpo@servertoday.com

Website www.servertoday.com

Phone 02-026-3112

Data Protection Officer

DPO Team

111/128 Moo 2, Ratchaphruek Rd., Bangraknoi, Mueang Nonthaburi, Nonthaburi 11000

Email dpo@servertoday.com

Phone 02-026-3112

10. Governing Law

This policy is governed by and interpreted in accordance with Thai law. Thai courts shall have jurisdiction over any dispute that may arise.

11. Policy Updates

The Company reserves the right to change and amend this policy. Please visit this website periodically to review the policy, as well as other information that the Company will update on its website. Where appropriate, the Company may notify you of any changes via the email you have provided.

This policy is effective as of May 6, 2025