



Gati Kintetsu Express Pvt Ltd

CIN: U62200MH2007PTC390900

Regd. Office: 4th Floor, A Wing, Allcargo House, CST Road, Kalina, Santacruz (East),
Mumbai - 400 098, Maharashtra

Website: www.gatikwe.com

Phone: +91 22 66798100

Information & Cybersecurity Policy

Commitment to Information Security

GKE recognizes that information is a critical business enabler in logistics. As we strive forth to maintain a leading position in our industry, we must always keep in mind the importance of the confidence of our stakeholders that include our customers, Gati'ites, and shareholders. Protecting the information assets from loss, theft, destruction, unauthorized modification and access, through implementation of Information Security, is one such critical measure.

The Information Security Policy (ISP) has been drawn up to set out the Management's strategy to address Information Security concerns and the responsibilities of Gati'ites to prevent breaches of security and thus protect our business. There are several controls which are being implemented across board aligning our organization with industry best practices to ensure a secure environment to store, process and transfer information. As Gati'ites, we need your utmost support to make this initiative a success. You will be aware that you are required to maintain confidentiality of all organization's information. This requirement extends to protecting organization's information stored on computer systems or otherwise in your possession and hence you are responsible for the security of such information whilst in your custody. Furthermore, we will provide the necessary guidance and support to ensure that all aspects of this Information Security Policy are successfully implemented.

Scope

The management of GKE ensures that Information Security is promoted, implemented and managed consistently by establishing a dedicated Information Security organization, who defines standards and supporting processes, which are instantiated and implemented throughout Gati. Information Security at Gati aims to protect all assets belonging to Gati from Information and cyber security related threats. This includes, but is not limited to, customer data, financial data, and employee data, applications, storage and computing devices, networks, and physical assets. The Policy is applicable to all employees, contract workers, contractors, vendors, suppliers and Members of the Board (hereby collectively referred to as "employees") across all subsidiaries and joint ventures of GKE.

Within Gati, Information Security objectives are:

- To ensure and provide adequate Information Security guidelines for implementing controls and processes necessary to safeguard and protect Gati data.

- Ensure that employees understand their roles and responsibilities regarding information security and data protection.
- Reduce number of adverse incidents, proactive response to any contingency & recovery of identified critical activities within agreed timeframe.
- Adherence to legal, statutory, contractual and regulatory requirements

Information Security Framework

The policy complacent requirements of customers, document continual improvement of the security posture to protect the information of interested parties and motivate employees to fulfill the purpose of the policy. Through this, GKE ensures strengthening their existing bonds with its business partners, employees, management, and customers. GKE communicates the current information security management system, the information security policies and procedures to its employees, management and relevant interested parties.

Key Information Security controls

Threat and Vulnerability management

- We are committed to maintain organization and its systems confidentiality, integrity and availability to maintain the trust and confidence of our customers. Therefore, the security of our online platforms and applications is of great importance to us.
- We have a robust threat and vulnerability management program implemented across the organization which focuses on identifying vulnerabilities within Operating systems, applications, and IT assets. We have internal & external scans performed at periodic intervals. We have documented process for vulnerability closures as part of our vulnerability management program.

Data Security

- Gati responsibly manages stakeholders data that includes its customers. GKE is reliant on data as a key enabler in digitally integrated offerings. We ethically manage, protect, and control the storage data to avoid any abuse and privacy breach. We have ensured to continually safeguard our position from legal, business and reputational risks.
- In Gati, we collect and process data only which is necessary for the business purpose. Data is handled in a transparent manner with due respect for the choices

and fundamental interests of our customers, business partners, and employees. Through cross functionally anchored governance, we ensure technologies and data are used to innovate and further optimize our services, sustainability initiatives and operations, while being compliant to regulations and adhering to high ethical standards

Physical and Environmental Security

- In GATI critical or sensitive information processing facilities are housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls. They are physically protected from unauthorized access, damage and interference. The protection provided is commensurate with the identified risks. The premises entry exits points and especially the critical areas are monitored by CCTV cameras. .

Information Security Incident and Cyber crisis management

- Our security Operations center operates 24/7 using a follow-the-sun model to continuously monitor our networks and provide rapid incident response. Controls are implemented for quick, effective, consistent, and orderly management of information security incidents including communication on security events and weaknesses. We have ensured information security events are handled through formal analysis, reporting, and escalation procedure. GKE mandatorily report cyber incidents/data breaches to its management and relevant interested parties.

Business Continuity

- GKE provides structured and robust strategy that ensures business recovery, personal safety, and adherence to regulatory and client requirements. We have defined & developed the objectives of this Policy test and maintain structured and coherent arrangements for enabling GKE to identify, communicate and respond to incidents in an effective and appropriate manner to minimize and eliminate the impact.

Privacy & Compliance

- In GKE privacy and protection of personally identifiable information are confirmed as required in relevant legislation and regulations where applicable. GKE has implemented appropriate technical and process control measures to protect personally identifiable information as identified in the risk assessment. The controls

address mechanism for ensuring that information is obtained and processed fairly, lawfully and properly. It also ensures information is accurate, complete and up-to-date, adequate and relevant. Personal records are maintained & stored securely. GKE has ensured appropriate weeding & deletion of information controls are in place. GKE communicates and notifies its employees and relevant interested parties in case there is a change in policy.

Should you require any further information regarding the GATI KWE Information security policy, please contact the Corporate Information security team at itsecurity@allcargologistics.com.