# Information and Communications Security Policy

Getac Technology Corp. (hereafter as Getac) top management formed “Getac Group Information and Communications Security Policy”, Getac Inc. (hereafter as GUSA) shall comply with the policy to protect the company's critical information assets confidentiality, integrity, and availability from internal or external deliberate or accidental damage; also, this policy is compatible with the strategic direction of Getac、relevant laws and regulations、information security needs for business and operation activity and contractual requirements.

A 2018/07/31 1. Initial Release.
B 2019/11/1 1. Modify content to be in line with HQ released SOP.

2. Scope of Application：
This “Information and Communications Security Policy” sets out the information security requirements to be followed, as well as role and responsibility for planning information security practices and continuing improvement.
The scope is as follows：
2.1 Organization and Personnel：
Including but not limited to Getac Group employees and external entity, service providers.
2.2 Information Assets-Hardware Assets：
All host, server, and moveable devices including but not limited to personal computers, terminal devices, communication devices, electronic media, storage media, and other related hardware assets.
2.3 Information Assets-Software Assets：
Business operation related application systems, software packages, and other related software assets.
2.4 Information Assets-Document Information Assets：
All business related data and information in electronic or paper formats.

3. Definition of Terms：
3.1 Information：
Including but not limited to, information displayed or stored in any form, unprocessed raw information, processed information, and intellectual properties /converted knowledge. Information is an asset, and like other important corporate assets, it is valuable to the organization and requires proper protection.
3.2 Information Security：
The purpose of Information Security is to ensure the confidentiality, integrity, and availability

of information. In addition, information security may include other properties, such as authenticity, accountability, non-repudiation, and reliability.

3.3 Confidentiality：

Characteristic of Information；Information is not made available or disclose to unauthorized personnel, entity, and process.

3.4 Integrity：

Characteristic of Information；It is to protect information accuracy and completeness.

3.5 Availability：

Characteristic of Information；Information is available and it is accessible and usable when an authorized entity demand access.

3.6 External entity, service provider：

Generally refers to organizations, agencies, or personnel outside of Getac Group, including but not limited to, competent authorities, software/hardware suppliers, external consultants, cleaning personnel, janitors, and security guards.

3.7 Information Security Indicator：

There should be documentation explaining how to measure the effectiveness of control mechanisms; that clearly defines when and how to measure the control mechanism; and demonstrates how to produce comparable and reproducible results. Information Security Indicator should cover three aspects: confidentiality, integrity, and availability, and should be properly integrated with the Information Security Policy statement.

3.8 ISMS：Information Security Management System.

4. Reference：

4.1 Getac relevant information security standard operating procedures and policy.

4.2 Personal Data Protection Act (Getac)

4.3 General Data Protection Regulation (GDPR)

5. Procedure：

5.1 Information Security Management：

For information security management purpose and to enhance employees' information security awareness, Getac has formulated information security control mechanism and the scopes as following,

5.1.1 Organization of Information Security

5.1.2 Management of Information Assets and Risk Assessment

5.1.3 Internal Audit on Information Security and Management Review

5.1.4 Management of Corrective Action

5.1.5 Management of Physical and Environmental security

5.1.6 Management of Network Information Security
5.1.7 Manage Information Security of Personnel and Information security awareness training
5.1.8 Management of Access Control
5.1.9 Management of Information Security in Supplier Relationships
5.1.10 Management of Information Security Incident
5.1.11 Management of Business Continuity
5.1.12 Information System Acquisition, Development and Maintenance
5.1.13 Information security in project management
5.1.14 Management of Information Backup and Recovery
5.1.15 Management of Technical Vulnerabilities and Control against Malware
5.1.16 Protection of personal data and privacy
5.1.17 Management of Information Regulation and standard operating procedure compliance

5.2 Management of Documented Information：

5.2.1 Creating and updating：

When Creating and updating relevant ISMS document, GUSA shall ensure appropriate reviewed and approval for suitability and adequacy.

5.2.2 Control of documented information：

Relevant ISMS document shall be controlled to ensure available and suitable for use, where and when it is needed; also, it is adequately protected.

5.3 Other Information Security Managing Items：

GUSA shall evaluate the information security performance and the effectiveness of ISMS, standard operating procedure shall be documented as reference for monitoring, measurement, analysis and evaluation.

5.4 Periodically Assessment

The “Information and Communications Security Policy” will be assessed by the Getac management meeting that is held annually. The policy could also reassess the adoption of changes in information security laws and regulations, technology and business operation newest development.

It is to ensure ISMS continuing suitability, adequacy and effectiveness.

5.5 Implementation

Before the policy is published, it must be approved by the chairperson of the information security committee, GUSA shall update accordingly. This policy implementation is effective from the release date.

6. Responsibility:

6.1 Information Security Committee

The Information Security Committee shall be the highest guidance and arbitration unit for the Getac Group's information security.
The Information Security Committee is responsible for guiding the direction of the information security policy, as well as supervising, researching, planning, implementing, and coordinating various information security related matters.
6.2 All Employees of the Getac Group
All employees should understand and comply with this “Information and Communications Security Policy”.
All employees have obligation to participate in annual information security training, and training records shall be included in performance appraisals.
All employees should assist external units and personnel in understanding and effectively complying with this “Information and Communications Security Policy”.

7. Appendix:
Getac Group Information and Communications Security Policy Statement

To maintain the security of information in the operating environment of Getac Group, our company is committed to fully protecting and preventing company and personal information from damage, theft, leakage, tampering, abuse, and infringement. Getac Group formulates Information and Communications Security Policy and shall be enforced to each relevant business functions and levels. The methodology of Plan-Do-Check-Act is adopted for promoting information and communication security continual improvement; it is preserving confidentiality, integrity, and availability of information security to give confidence to interested parties that risks are adequately managed.

The Getac Group's Information and Communications Security Policy is as follows:
1. All employees of the Getac Group and external personnel shall abide by the Information and Communications Security Policy and relevant safety regulations. If a violation occurs, Getac Group will enforce the violator’s legal and contractual responsibilities according to the circumstances; employees of the Getac Group may be penalized in accordance with relevant HR protocols.
2. Personal identifiable information from employees, third party vendors, and customers are entitled from the protection of applicable laws and regulations of privacy and personal information protection；Personal identifiable information shall not be used until the individual's consent is obtained. All other information assets are owned by the company.
The Getac Group has the right, in accordance with applicable law, to check, store, transfer, exchange, and copy such information assets.

3. All employees of the Getac Group and external unit personnel, who use any of the Getac Group’s information assets, have the responsibility and obligation to prevent unauthorized access, tampering, destruction, and improper disclosure. All Getac group information assets should be accessed and used in accordance with the Getac Group's information security regulations.
4. Getac Group Employees are obliged to protect trade secrets and intellectual property learned from operations. It is strictly forbidden to disclose trade secrets and intellectual property information to colleagues, manufacturers, and other personal who are not related to the business.
5. It is strictly forbidden for all personnel to install, use, or download illegal or unauthorized software on the company's information assets.

6. In order to safeguard Getac Group's business related data, the Getac Group must properly identify each employee’ s job responsibilities and segregation of duties；only grant the necessary authority and information to complete the employee’ s work.
7. All personnel, Getac employees and its external service providers, should be alert at all times to information security incidents and violations of security policies and procedures, and should promptly notify the Getac Group’s local Information management unit in accordance with the procedures.
8. The Getac Group shall establish a continuous operation plan in according to business needs and annually exercise the drill to maintain its applicability.

Maintaining Information and Communications Security is of utmost importance. All units should have a clear understanding of the Information and Communications Security policy and should follow the relevant regulatory procedures to maintain information security and sustainable operation of all of Getac Group's businesses.