

Information Security Management System (TISAX) Policy

Bangchan General Assembly Co., Ltd

1. Introduction

Bangchan General Assembly Co., Ltd. (hereinafter referred to as "BGAC") recognizes the utmost importance of information security in business operations, especially as an Automotive General Assembly Manufacturer working with world-leading companies such as BMW and Mercedes-Benz. This policy is developed to align with the TISAX (Trusted Information Security Assessment Exchange) standard and to strictly protect important information of the company and customers, as well as to comply with relevant laws such as the Cybersecurity Act and laws protecting personal data of employees and relevant stakeholders.

2. Objectives

- 2.1 To establish guidelines for maintaining the security of BGAC's information systems.
- 2.2 To ensure that BGAC and customer data, especially BMW and Mercedes-Benz, are protected as strictly and appropriately as possible.
- 2.3 To build maximum confidence with customers and business partners in data security.
- 2.4 To comply with TISAX standard requirements and improve processes related to information system management.



บริษัท บางชันเจนเนอรัลแอสเซมบลี จำกัด
BANGCHAN GENERAL ASSEMBLY CO.,LTD.
99 SOI SERITHAI 56, KANNAYAO, BANGKOK 10230 THAILAND
TEL. 02-5170022-7, FAX. 02-5181485, 02-5179551, 02-5170628 P.O.BOX. 24-5 BANGKOK 10240
Website : www.bgac.co.th E-mail : info@bgac.co.th



3. Scope

This policy covers all information systems, equipment, personnel, and processes related to BGAC's data management that are involved in operations for European customers such as BMW and Mercedes-Benz, which require compliance with the TISAX standard. This includes protecting personal data of employees, subcontractors, and third parties who access company and customer data.

4. Core Information Security Management System Policies

4.1 Information Asset Management

BGAC will create and maintain an up-to-date inventory of information assets, with special emphasis on customer-related data. Owners and responsible parties will be assigned for each information asset, especially data related to BMW and Mercedes-Benz. Secure passwords will be used for data storage devices to prevent data leakage and unauthorized access.

4.2 Access Control for Information Systems (Employees and Subcontractors)

Strictly apply the Principle of Least Privilege. Regularly define and review access rights, especially for data related to new products or confidential customer information. Enforce Multi-Factor Authentication for critical systems and VPN for remote access. Subcontractors will be granted access rights according to the scope of their contract and must sign a non-disclosure agreement before starting work.

4.3 Physical Security and Operations

Restrict access to important areas (Security Control Areas) with access control systems. Install Access Control systems at entrance doors along with CCTV systems. Designate responsible persons for alerting in case of unauthorized intrusion. Define safe operating procedures for all information systems, with special emphasis on systems related to customer data. Regularly inspect and improve systems.



บริษัท บางจันยานเนอโรอเชมบิล จำกัด
BANGCHAN GENERAL ASSEMBLY CO.,LTD.
99 SOI SERITHAI 56, KANNAYAO, BANGKOK 10230 THAILAND
TEL. 02-5170022-7, FAX. 02-5181485, 02-5179551, 02-5170628 P.O.BOX. 24-5 BANGKOK 10240
Website : www.bgac.co.th E-mail : info@bgac.co.th



4.5 Communication Security

Encrypt all important data transmitted over networks, especially data related to BMW and Mercedes-Benz. Use highly secure VPNs for remote system access. Conduct technical vulnerability assessments to reduce risks arising from both internal and external communications.

4.6 System Acquisition, Development, and Maintenance

Review security requirements in the process of developing and purchasing software systems and related equipment, considering security needs for customer information. Conduct security testing before implementing new systems and maintain system efficiency throughout its use.

4.7 Information Security Incident Management

Establish a capable Incident Response and Business Continuity Team, using external contractors to manage abnormal incidents. Define incident reporting and management procedures, giving highest priority to incidents that may affect customer data and sensitive personal data of employees. BGAC has a policy to strictly comply with all relevant laws and regulations, conducting regular internal audits to ensure compliance with TISAX policies and standards.

5. Protection of Customer Data and New Products

5.1 Customer Data Management

Set the highest security level for BMW and Mercedes-Benz data. Limit access to customer data to only those who need to know. Monitor and record every access to customer data (Log Management).

5.2 Confidentiality of New Product Information

Establish measures for managing information about new products, especially unreleased car models. Use encryption systems for all new product data. Restrict access to areas where new products are developed or tested. Prohibit the use of personal devices in areas where new product data is handled.

5.3 Training

Provide training related to information system security for employees who access confidential data, customer data, and new product-related data to raise awareness of the importance of confidentiality. Emphasize the importance of protecting customer data and new products, as well as preventing cybersecurity risks and threats from employees.

6. Review and Improvement

Review and update this policy at least annually or when there are significant changes in the industry or customer requirements. Conduct annual information security risk assessments, with special focus on risks related to customer data and new products.

7. Enforcement

All employees, subcontractors, and third parties accessing BGAC's information systems must strictly adhere to this policy. Violations of the policy, especially regarding the protection of customer data and new products, will be considered serious offenses.

Penalties for policy violations may include:

- Warning and suspension of system access rights
- Disciplinary action
- Termination of employment or contract
- Legal action in cases of serious damage

8. Security Breach Reporting

All employees have a duty to immediately report any security breaches or suspected breaches. Provide safe and confidential reporting channels. Protect whistleblowers who report in good faith.

9. Customer Coordination

Establish special communication channels with BMW and Mercedes-Benz for data security issues. Report progress in complying with TISAX standards to customers. Coordinate closely with customers in case of policy changes or security measures that may affect customer data.

10. Certification and Auditing

Work towards obtaining and maintaining TISAX certification continuously. Prepare for and cooperate in audits from external agencies and customers. Use audit results to continuously improve the security system.

11. Approval and Dissemination

This policy has been approved by BGAC's executive committee and is effective from 9 Sep 2024. This policy will be disseminated to all employees, subcontractors, and relevant third parties. A shortened version will be created for internal and external communication as follows:

BGAC

B - Beware of data breaches

G – Guard customer information

A - Always follow security protocols and procedures

C - Confidentiality is key

Signed: _____

Vunchai Jungsanguanpornasuk

President & CEO

BANGCHAN GENERAL ASSEMBLY CO., LTD.

Date: [9 Sep 2024]