SUPPLIER INFORMATION SECURITY POLICY

- Protection of the integrity, confidentiality and usability of the information shared by the supplier and/or (sub)contractor with our institution,
- With the services received from the supplier and/or (sub)contractor, the healthy operation of the information systems infrastructure and the continuity of all kinds of works and transactions carried out,
- Protecting the confidentiality of our corporate and personal information shared with confidentiality and non-disclosure agreements,
- Compliance with legal and regulatory requirements, including data protection, intellectual property rights and copyrights, within the scope of the service,
- Goods and service procurement contracts include agreed terms such as maintenance/repair conditions, solution time, response time, supply time, and penal clauses if the aforementioned conditions are not met,
- Performing risk analyzes in cases where confidentiality and non-disclosure agreements cannot be signed, agreeing on the measures to be taken with the supplier,
- The use of secure information transfer methods between our institution and the Supplier, the handling of information transfer rules in contracts, the use of methods approved by our institution,
- Adapting to the differences that may be caused by the innovations and changes that may occur in the legislation (laws, regulations, communiqués, circulars, etc.)
- Using secure remote access methods for remote access to information systems, recording and reporting of remote access activities, using methods approved by our institution
- Recording supplier-based Information Security violations that occur during service procurement
- Taking protective measures against threats arising from security vulnerabilities of systems used by suppliers and/or (sub)contractors for remote access during service procurement,
- Regular evaluation of suppliers with information security criteria and sharing the evaluations with suppliers,
- Increasing the Information Security awareness of suppliers by organizing Information Security Awareness Trainings and Information Security audits when needed
- Notifying our institution as soon as possible and agreeing on any changes (personnel changes, version updates, hosting condition updates, etc.) that will occur in the products or services provided by the supplier and/or (sub)contractor.

PHI Metal Otomotiv Sanayi ve Ticaret A.Ş.

Executives