•APTIV•

Third Party Security Requirements Standard

Document Type: Standard Document
Document Reference Number: ECS_SEC.STD
Review Period: Annual, every 12 months from the last approval.

Document Management

Author: George Szabados, Manager, Third Party Security Risk Management
Owner: George Szabados, Manager, Third Party Security Risk Management
Approver: Jonathan Shih, Director Risk Compliance & Resilience

Revisions Log

Version	Date	Named Person	Activity Description
1.0	January, 2019		Initial Release
1.1	January, 2020		Updated document
1.2	June, 2021		Updated with additional controls for vendor compliance and security
1.3	January 21, 2025	George Szabados, Third Party Risk Management	Updated with TPRM information, revised controls and updated template

Approvals and Signatures

Document approval for the standard to go into effect, and hereinafter for each revision and periodic review.

Document Owner	*George Szabados*
	George Szabados, Third Party Risk Management
	January 15, 2025

Approving VP or Department Head	*Jonathan Shih*
	Jonathan Shih, Director Risk Compliance & Resilience
	January 21, 2025

APTIV

Table of Contents

Introduction

Aptiv security policies cover the management of security for both Aptiv internal operations as well as the services Aptiv provides to its customers.

Aptiv Cybersecurity policies are classified as Aptiv Internal and are not available for review by Customer or third parties. However, this standard is a requirement for the engagement of Third-Party Service Providers are provided below.

Lack of inclusion or omission of a subject in this standard does not eliminate oversight and responsibility on behalf of the Third Party, and they are expected to exercise due care and sound judgment and recognize potential Information Security concerns or risks.

Aptiv expects evidence ensuring this standard is met and will be provided upon request. As part of Aptiv vendor governance, in particular for medium to high-risk vendors, annual compliance checks are performed by Aptiv, to validate ongoing compliance by the vendor with the controls, standards and requirements as per contract agreements.

Any questions with respect to information security guidance or practices, should be immediately directed to Aptiv's Cyber TPRM Team at enterprisecybersecuritytprm@aptiv.com email address.

Any vendor concerns of potential security incidents either within Aptiv, or in our vendors which has the potential to be a risk to Aptiv must be reported immediately to Aptiv Security Operations Centre SOC@aptiv.com

Scope

This standard applies to Third Party companies globally, including visitors, contractors, and suppliers; providing any services to Aptiv which can include but is not limited to:

- The creation of, purchase of, or right to use software, web applications, IT utilities, IT services and/or hardware
- the capture, storage, or transfer of Aptiv data, whether standalone by the supplier, between Aptiv and the supplier, or between third parties
- delivery of outsourced services such as support services, managed services, software development, supplying contractors

These requirements also apply to all information systems owned, contracted, leased or operated for or by Aptiv, connected to the Aptiv network, or used to process, stored, or transfer Aptiv data.

Summary for Third Party companies

Aptiv computing and data communications are valuable and limited resources that serve a large number and variety of users. (NOTE: A “user” is any Aptiv person, including: permanent/full- time employees, temporary employees, contractors, and any other individual that is working with or on behalf of Aptiv, and/or has access to Aptiv information or resources.)

All users have the responsibility to make use of these resources in a secure, efficient, ethical, and legal manner.
Aptiv reserves the right to conduct security scans and monitor system access and use, as part of security and compliance processes, to ensure appropriate and legitimate use of Aptiv assets.

Aptiv’s computer and network services provide access to resources both within and outside the Aptiv environment. These services must be used in a manner consistent with the mission and objectives of Aptiv and with the purpose for which such use was intended. Such access is a privilege and imposes upon users’ certain responsibilities and obligations. Access to Aptiv's Assets (computers, applications, network services and data) is granted subject to Aptiv policies, and applicable laws.

Acceptable use is always ethical, reflects professional integrity, and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property, protection of sensitive information, ownership of data, copyright laws, system security mechanisms, and individuals' rights to privacy and to freedom from intimidation and harassment.

All activities inconsistent with these objectives are considered to be inappropriate and may jeopardize continued use of computing facilities and networks.

In consideration of being allowed to use the Aptiv Resources, all users must understand and agree to the following:

1. Users shall not use the Resources for any illegal activity or for any activity prohibited by this policy (see subsequent examples of inappropriate conduct that is prohibited).

2. Users agree not to use the Resources to infringe upon or otherwise impair, interfere with or violate any copyright or other intellectual property rights of another. This pertains to all Aptiv intellectual property as well as copyrighted material, including, but not limited to music, video and software.

3. Users shall avoid any action that interferes with the efficient operation of the Resources or impedes the flow of information necessary for conduct of Aptiv business.

4. Users shall protect Aptiv resources such as ID, logins and systems from unauthorized use. Users are responsible for reasonably securing their computer, including implementing such protections as logins to prohibit unauthorized use.

5. Users will access only information that is their own, or to which their access has been authorized. Users will only access networks, network resources, and information for their intended use.

Examples of inappropriate use of resources include, but are not limited to:

- Accessing another person's computer, computer account, files, or data without permission.
- Using the Aptiv network to gain unauthorized access to any computer system.
- Using any means to decode or otherwise obtain restricted passwords or access control information.
- Attempting to circumvent or subvert system or network security measures. Examples include creating or running programs that are designed to identify security loopholes, to decrypt intentionally secured data, or to gain unauthorized access to any system.
- Engaging in any activity that might be purposefully harmful to systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, damaging files or making unauthorized modifications to Aptiv data.
- Performing any act, intentionally or otherwise, that will interfere with the normal operation of computers, peripherals, or networks.
- Making or using illegal copies of copyrighted software, storing such copies on Aptiv systems, or transmitting them over Aptiv networks.
- Harassing or intimidating others via electronic mail, news groups or Web pages.
- Initiating or propagating electronic chain letters.
- Initiating or facilitating in any way mass unsolicited and unofficial electronic mailing (e.g., "spamming", "flooding", or "bombing.").
- Forging the identity of a user or machine in an electronic communication.
- Saturating network or computer resources to the exclusion of another's use, for example, overloading the network with traffic such as emails, excessive file backup/archive, or malicious (denial of service attack) activities.
- Using Aptiv systems or networks for personal gain; for example, by selling access to your ID or to Aptiv systems or networks, or by performing work for profit with Aptiv resources in a manner not authorized.
- Engaging in any other activity that does not comply with the general principles presented above.

Vendor Assessment Considerations

The following list intends to serve as considerations for assessing the risks associated with service providers' and third party's information technology practices, processes and controls. It presents a core scope of domains, with expectations of good security practices within those domains.
As it relates to Aptiv expectations for Vendor security, Aptiv will expect that the vendor will

- Act diligently when handling Aptiv information
- Implement best practices in relation to information security based on established security standards, such as TISAX, ISO/IEC 27000, NIST or equivalent.
- The ability to demonstrate accreditation or alignment with a recognized information security without major deficiencies.

While the specific controls and requirements can vary considerably with the nature or scope of the service, the following serves as a foundation to understand and manage the service providers' and third party's risks. The specific controls and amount of evidence required around those controls can also vary considerably with the nature and scope of the service provided and will be determined on a case-by-case basis, when Aptiv is completing its Third Party Risk Assessment processes.

SECURITY POLICIES	
Expectations:	All vendors and Service Providers should have and adhere to a written and comprehensive set of information security policy documents, which act as the rules and guidelines for dealing with the protection of information and information assets.
Evidence that may be requested:	• Security Policy Management System • Procedures and/or standards supporting the policy • Evidence of policy review • Audit report of security policies and controls • Implementation of best practices security processes and controls • Evidence of organisational and/or services/products security certifications / compliance or alignment with same • Security assessments findings
ORGANISATION OF INFORMATION SECURITY	
Expectations:	A management framework should be established to initiate and control the implementation of information security within the Service Provider's organisation. The Service Provider should have a process to review all dependent Service Providers' security policies and procedures to ensure that appropriate security language is incorporated into all third-party agreements.

Evidence that may be requested:	• Information security organisation chart (including where information security resides in the organisation) • Defined security Roles and responsibilities • Third-party security reviews/assessments, in particular for solutions or technologies leveraged by Aptiv or used by the vendor is their service delivery to Aptiv • Due diligence performed on third parties • Risk Management processes
ASSET MANAGEMENT	
Expectations:	Service Providers should have in place an appropriate asset control policy structure, including appropriate ownership, management, licensing and other controls that address the asset types including, but not limited to information assets, software assets, physical assets, and services. The information and materials processed, stored or transmitted by the Service Provider should be handled in accordance with the classification (e.g., confidential, sensitive, public) of the information.
Evidence that may be requested:	• Asset control policy • Information classification policy • Central Asset Management database • Timely return of any Aptiv asset for vendor's users no longer working with Aptiv
HUMAN RESOURCES SECURITY	
Expectations:	Service Providers should have and adhere to policies and procedures in place to perform background checks for those individuals who will be administering systems or have access to Aptiv's information. These policies and procedures should ensure that personnel responsible for design, development, implementation and operation are qualified to fulfil their responsibilities. All employees of the Service Provider's organisation, and where relevant, third-party users, should be made aware of security threats and concerns, their role and responsibilities as it relates to security, and should be equipped to support the organisational security policies in the course of their normal work.
Evidence that may be requested:	• Employment policy • Non-disclosure agreements • Third Party Agreements • Background check documents for staff supporting very sensitive services or data

PHYSICAL AND ENVIRONMENTAL SECURITY	
Expectations:	Business information processing, storage or distribution facilities should be housed in secure areas, protected by a defined security perimeter, with appropriate security barriers and entry controls. Facilities should be physically protected from unauthorized access, damage and interference. Access should be logged, and logs should be securely maintained. Equipment should be physically protected from security threats and environmental hazards in order to prevent loss, damage or compromise of assets and interruption to business activities.
Evidence that may be requested:	• Badge control policy • Physical access logging policy • Evidence of security logs • Physical access security and monitoring controls
COMMUNICATIONS AND OPERATIONS MANAGEMENT	
Expectations:	Responsibilities and procedures for the management and operation of all information-processing facilities should be established and adhered to. This includes the development of appropriate operating instructions and change control and incident-response procedures. Segregation of duties and environments (development, testing, staging and production) should be implemented where appropriate to reduce the risk of negligent, inadvertent or deliberate misuse of information-processing facilities and systems. Controls should be in place to prevent and detect the introduction and dissemination of malicious software. Recovery plans should be prepared, updated and tested regularly. Routine backup procedures should be established and adhered to for carrying out the agreed backup strategy, such as taking backup copies of data, rehearsing their timely restoration, logging events and faults, and, where appropriate, monitoring the equipment environment.
Evidence that may be requested:	• Network security controls • Endpoint Protection • Email Security controls • SOPs (standard operating procedures) • Operations (network, processing) and incident response team organisation charts • Security Education procedures & material • Change control process • Backup policy and processes • Incident identification and response process • Test plans and results

	• Third-party due diligence records and contracts • Planning and acceptance records • Dataflow diagram
ACCESS CONTROL	
Expectations:	Service Providers should have and adhere to a documented policy, and effective procedures, for the management of user identities and their access. This is to ensure that only properly approved users are granted access to systems and assets, and that access is removed as soon as it is no longer required. For example, when an employee's contract is terminated. Users should be granted access on a need-to-know basis, according to job responsibilities. The access-control policy should employ methods designed to physically and logically restrict access to assets, ensure the identification and authentication of individuals who access computing resources and restrict an individual's access to information once the individual has accessed a system. Depending on the level of protection required (based on the asset classification); a combination of access control techniques may need to be employed. Users should be aware of their responsibilities for maintaining effective access controls, particularly as they relate to password security and user equipment. Service Providers should have a written authorized user accountability policy that incorporates authentication standards and clearly articulates user responsibilities.
Evidence that may be requested:	• Password Policy • Identity & Access management controls • Auditing & Logging of access requests and approvals • Application access control procedures • Bi-monthly reviews performed by vendor, of any Aptiv accesses to verify access is still required • Timely termination of Aptiv accounts used by vendor's users who no longer need access (no longer on Aptiv account, or no longer working with the vendor)
INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE	
Expectations:	Service Providers should have and adhere to an established process for developing secure infrastructure, systems, and/or applications. Products and services developed should be certified as free from malicious code and patent-infringement issues and appropriate for use. The programs should also be protected from unauthorized copy, use, duplication, and storage, with asset-management requirements specified. Service Providers should ensure all proposed system changes are reviewed and tested to be sure they do not compromise the security of either the system or the operating environment.

Evidence that may be requested:	• Application security policy • Secure Development Lifecycle • Programming standard and guidelines • Certifications of encryption algorithms • Documentation of security reviews of application code • Vulnerability assessments of application and environment (including cloud) • Reviews of known vulnerabilities in hardware or software • Evidence that vulnerabilities are remediated or required approval by Aptiv based on vulnerability assessment
INFORMATION SECURITY INCIDENT MANAGEMENT	
Expectations:	Defined policy and processes for security incident detection, investigation and response. Security events and vulnerabilities associated with information systems are communicated in a manner allowing timely corrective action to be taken. A consistent and effective approach is applied to the management of information security incidents.
Evidence that may be requested:	• Incident management and response policies and procedures • Security Incident Management team or service • Volume of High threshold security incidents in the last 12 months • Security Operation tools used, such as SIEM, vulnerability scanning, incident management platform etc. • Log of incidents with evidence of investigation procedures and results • Reporting of security incidents to Aptiv, from security incidents within Aptiv that the vendor is aware of, or a vendor incident which may pose a risk to Aptiv in any way.
BUSINESS CONTINUITY MANAGEMENT	
Expectations:	Service Providers are expected to have business continuity plans for key systems that may impact business operations or quality of service, if the systems are impacted by an event e.g., cyber-attack, loss of power, hardware failure. BCP controls can include high availability capabilities or DR processes or solutions to ensure efficient recovery of services during a time of business interruption. These plans should be tested at least annually, and results of the tests documented. The Service Provider is responsible for ensuring its suppliers have appropriate business continuity programs to meet its business requirements and SLAs and that those plans are included in recovery testing
Evidence that may be requested:	• Business continuity plan • Disaster Recovery plan

	• Testing DR, processes, backup and recovered schedule and/or results
COMPLIANCE	
Expectations:	Service Providers should establish and adhere to policies to ensure compliance with applicable legal and regulatory requirements. These requirements should reflect any international environments that must be accommodated based on processing locations. Information systems should be audited regularly for compliance with the Service Provider's security policies and standards.
Evidence that may be requested:	• List of compliance standards applicable to the organisation • Third-party assessment reports • Regulatory reports • Annual reports (if a publicly traded company) • Financial statements for prior two years (audited, if available) • Provide annual evidence of compliance with specific standards or certifications the vendor is required to hold, as part of Aptiv contracts.
CYBERSECURITY CULTURE	
Expectations:	Service Providers should establish and maintain an ongoing security training and education to their employees, to ensure awareness of organisational security policies, current threats, how to act security and how to respond and report in the case of a suspected incident
Evidence that may be requested:	• Information Security training of employees • Phishing test results • Security and/or technical certification of employees in accordance with their responsibilities • Completion of assigned Aptiv Information Security training for vendors supplied resources who have an Aptiv ID and access