SECURITY REQUIREMENTS - SERVICES

Definitions

On-Site services : Services provided by a Supplier working on a Client (or the Client's customer) site and accessing Client's (or the Client's customer) information system.

Off-site service : Services delivered by a Supplier from Supplier's site:

- **connected to Thales IS :** accessing Client's information system: (i) with a dedicated and secure area for Client only, or (ii) from their premises with compliancy to Thales Security Rules.
- **not connected to Thales IS :** Services delivered by a Supplier from the Supplier's site, without accessing Client's information system**.**

Thales Asset: (i) any non-tangible asset of the Client, such as files, data received and processed and deleted and/or data of the Client, which is used for the performance of the Services, and/or (ii) any tangible asset of the Client which is used, transformed or/and transferred in the context of the Services.

Security Incident: a breach of security leading to a successful or an imminent threat of (i) unauthorized or unlawful access, use, disclosure, modification, theft, loss, corruption/alteration or destruction of data belonging to Client (or the Client's customer) (ii) interference with information technology operations, or (iii) interference with system operations.

Information security policies

The Supplier ensures that it has developed and implemented, and will maintain and monitor, a written and comprehensive information security policy (the "security policies") which includes in its scope the sites, activities, personnel and systems used to develop or deliver the Services (e.g. ISO 27001, NIST). The security policies shall define:

- For an organization, the constraints on behavior of its members as well as constraints imposed by mechanisms such as doors, locks, keys and walls.
- For systems, the constraints on functions and flow among them; constraints on access by external systems including programs and access to data by people.

In case of Off-Site Services, the Supplier shall notify Client within one month any update of its security policies. In any event, the Supplier shall not decrease the security level of the Product or Services. Client may review relevant security policies and procedures at Supplier's site. The Supplier shall comply with the latest version of the Thales Protection of Group Information as communicated by Purchase, which is applicable to the services, products and IT technologies delivered in the course of and for the purpose of the performance of the Services or the delivery of the Products.

Organisation of information security

Before the performance of the Services, the Supplier shall communicate to Client its governance regarding security and cybersecurity including points of contact and their responsibilities and tasks.

Access Control

In case of Off-Site Services, the Supplier's assigned administrator(s) must retain sole responsibility for granting access to Thales Asset and to Thales Personal Data for all Supplier employees and other users, and for providing a process by which employee and other user accounts shall be created and deleted

in a secure and timely fashion. This process must include appropriate leadership approval, auditable history of all changes, and an annual review of access authorization and excess access remediation.

The Supplier shall establish, maintain and enforce the security access principles of "segregation of duties" and "dual control" and "least privilege" with respect to Thales Asset and Thales Personal Data.

In case of Off-Site Services connected to Thales IS, the Supplier submits to Client approval the identity of any Supplier's employee that will be granted with remote access privileges to the Client internally hosted IT components and networks. This applies in particular when the operation requires creating an account for a person on the Thales directory.

The Supplier shall register and keep the logs to any access to Thales Assets, Thales Personal Data and Thales information system by its staff, agents or sub-contractors, and that these logs shall be communicated to Client.

Asset / Thales Personal Data management

In case Off-site service not connected to Thales IS or connected to Thales IS, the Supplier shall establish and maintain administrative, technical and physical safeguards to protect the security, integrity, confidentiality and availability of Thales Asset and Thales Personal Data and, including to protect Thales Asset and Thales Personal Data against any anticipated threats, hazards, and to protect against any Security Incident.

The Supplier maintains an inventory of all Thales Assets (or of the components that support those Assets).

Physical and environmental security

In case Off-site service connected to Thales IS, the Supplier shall provide the geographic locations in which it operates Thales Assets and/or processes Thales personal data. In particular, the Supplier shall provide the address of its
a) Primary Data Centre and / or computer facility and
b) Backup and / or Disaster Recover Site.

In case of On-Site Services, the Supplier shall comply with the Prevention Plan communicated by Client and which is applicable to the Services and IT technologies delivered in the course of and for the purpose of the Services.

Operations security

The Supplier shall maintain a security environment designed to ensure that the Services are protected from malware. In particular, the Supplier shall:
a) use all care and means available to prevent intrusion of malicious code on its servers, workstations and all possible infrastructure (e.g. e-mail gateways, etc.);
b) implement detection, prevention and recovery controls to protect against malware for its systems. Applicable quarantine measures shall be enforced on infected network devices until they are cleaned;
c) ensure that anti-virus/anti-intrusion software engines, and their patterns/signatures databases, are updated regularly on all devices, including mobile ones.

The Supplier shall ensure that critical patches are applied to its systems as recommended by software vendors, and after being tested by the Supplier for compatibility with its installations.
Supplier agrees to maintain and enforce retention policies for any and all reports, logs, audit trails and any other documentation that provides evidence of security, systems, and audit processes and

procedures according to requirements mutually agreed upon by Thales and Supplier, one (1) year being Thales's standard retention requirement. Such retention period may change in accordance with all applicable laws and regulations.

In case of Off-Site Services, the Supplier agrees to employ supported software (e.g., software under active maintenance, including operating system, open source, application software and/or the like) on any systems that process, store or otherwise support the Services. The Supplier shall notify Client in advance (1 year) of any end of support of any component.

System acquisition, development and maintenance

Rules for the development of software and systems shall be established and applied to developments within the organization. At least, rules for software development shall include:
a) No hardcoded credentials shall be used
b) Administrator and user roles shall be separated
c) All default accounts used in the development process shall systematically be removed and the default password shall be changed before delivery to Client.

Supplier shall provide evidences of the following points concerning the design of its Services:
a) Cyber risks faced by the Services shall be identified and lead to the creation of appropriate cybersecurity controls to be put in place.
b) Trusted and untrusted data sources (for example, data sources internal to the Client's organization could be considered as trusted whereas other data sources might be considered as untrusted) shall be identified.

In case of Off-Site Services, the Supplier agrees to perform (at least annually) a vulnerability threat assessment test or such other testing of its systems that have access to or contain Thales Asset and Thales Personal Data and shall mitigate or remediate critical findings in a timeframe commensurate with the impact of the defect and the required implementation workload. Upon request, the Supplier agrees to provide Client with reports which may include a date of the test, who performed the test, and an indication of the relative risk of identified vulnerabilities, as well as a timeline to remediate any findings. The vulnerability threat assessment shall be performed using industry standard threat assessment tools and or services. The Supplier shall ensure an annual basis review and audit of its systems' security robustness. To do so, the Supplier will conduct periodic reviews of the security of its network and adequacy of its information security program as measured against applicable industry security standards and its policies and procedures.The Supplier will continually evaluate the security of its network and associated services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews. The Supplier shall identify, initiate, manage, record, report and close down all appropriate remedial/corrective actions in respect of any defects identified by any security audit, review, monitoring activity or incident, in a timeframe commensurate with the impact of the defect and the required implementation workload.
Client reserves the right to discontinue or restrict the connectivity or information access for the Supplier in the following cases:
a) Supplier refuses the Client to conduct a security audit
b) corrective actions are not implemented, or
c) lack of collaboration in case of a major Security Incident. Supplier shall implement a formal change control process for software and hardware Products. Information about technical vulnerabilities of information systems or components being used by the Supplier to provide the Services shall be

communicated to the Client in a timely fashion, the Client's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

In case of On-Site Services, the Supplier shall ensure an annual basis review and audit of its systems' security robustness. To do so, the Supplier will conduct periodic reviews of the security of its network and adequacy of its information security program as measured against applicable industry security standards and its policies and procedures.The Supplier will continually evaluate the security of its network and associated services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews. The Supplier shall identify, initiate, manage, record, report and close down all appropriate remedial/corrective actions in respect of any defects identified by any security audit, review, monitoring activity or incident, in a timeframe commensurate with the impact of the defect and the required implementation workload. Client reserves the right to discontinue or restrict the connectivity or information access for the Supplier in the following cases:

a) Supplier refuses the Client to conduct a security audit

b) corrective actions are not implemented, or

c) lack of collaboration in case of a major Security Incident.

Supplier Relationships

In case of Off-Site Services, the Supplier shall systematically use malware detection tools before delivery to Client and provide to Client the report of this malware detection.

Information Security Incident management

The Supplier shall implement a comprehensive and approved Security Incident management process for information and systems it operates, that includes identification, response, containment, recovery, reporting, evidence protection and post-implementation review of information Security Incidents.

The Supplier agrees to notify Thales CERT without undue delay, and in any event no later than 24 hours, upon learning of Security Incidents at the following address: CERT@thalesgroup.com. The notification shall include at least:
a) problem statemen t or description
b) expected resolution time (if known),
c) and the name and phone number of the Supplier representative that Client may contact to obtain updates.
Evidence relating to a Security Incident shall be collected, retained and presented by the Supplier to conform to the rules for evidence laid down in the relevant jurisdiction(s).

Information security aspects of business continuity management

In case of Off-Site Services, the Supplier shall have deployed the means to ensure business continuity and recovery in case of a disaster, including resilience of the Products or Services delivered to Client. The Supplier shall notify Client when a disaster occurs.

Compliance

In case of Off-Site Services, the Supplier acknowledges that Client or an independent auditor designated by Client, at its own expense, may audit and monitor to confirm the compliance with the

security agreements of systems, processes and procedures of the Supplier and its supply chain, relevant to the Services provided to Client or where Client systems or information may be placed or accessed from. This includes but is not limited to verifying information access approval and control, control of information flow, and audit trails. The Supplier will provide all relevant documentation and evidence. Due to the confidential and proprietary nature of the Supplier's operations, and in order to protect the integrity and security of the Supplier's operations and the shared nature of systems which may be used to provide the Services under the Order:
a) both Parties shall agree in advance the scope of such inspections,
b) a written notice of no less than 30 days prior to the anticipated start date of the inspection shall be given by the Client and may occur no more than once in any twelve (12)-month period, barring exigent circumstances, such as Client's reasonable concern of a Security Incident, in which case an inspection may be performed in response to such circumstance or concern, and at a time mutually agreed by both Parties.
c) if to be conducted by a third party, the third party must be a mutually agreed upon security assessment specialist, where such agreement by Supplier shall not be unreasonably withheld,
d) are subject to appropriate confidentiality and non-disclosure provisions, and
e) may not unreasonably disrupt Supplier normal business or IT operations.

Notwithstanding the foregoing, the Client retains the sole discretion as to whether to initiate a security review under this section, and may initiate such a review prior to production use of the Services and thereafter, (2) upon any change in the Services that could affect the security of any element thereof, (3) following any Security Incident affecting the Products or Services or Thales Assets or Thales Personal Data, and (4) upon Client's request or demand from a governmental body having jurisdiction. The Supplier shall provide Client with reasonable assistance as may be required to enable Client to comply with applicable laws in connection with any issues implicated by a security review.Evidence shall be kept and protected by the Supplier to prove compliance with contractual or applicable legal obligations and made available and delivered where necessary to Client.

SECURITY REQUIREMENTS - OFF THE SHELF HARDWARE

Definition

Security Incident: a breach of security leading to a successful or an imminent threat of (i) unauthorized or unlawful access, use, disclosure, modification, theft, loss, corruption/alteration or destruction of data belonging to Client (or the Client's customer) (ii) interference with information technology operations, or (iii) interference with system operations.

Organisation of information security

Before the delivery of the Products, the Supplier shall communicate to Client its governance regarding security and cybersecurity including points of contact and their responsibilities and tasks.

System acquisition, development and maintenance

Information about technical vulnerabilities of information systems or components being used by the Supplier to provide the Products shall be communicated to the Client in a timely fashion, the Client's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

The Supplier shall ensure an annual basis review and audit of its systems' security robustness. To do so, the Supplier will conduct periodic reviews of the security of its network and adequacy of its information security program as measured against applicable industry security standards and its policies and procedures. The Supplier will continually evaluate the security of its network and associated services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.

The Supplier shall identify, initiate, manage, record, report and close down all appropriate remedial/corrective actions in respect of any defects identified by any security audit, review, monitoring activity or incident, in a timeframe commensurate with the impact of the defect and the required implementation workload.

Client reserves the right to discontinue or restrict the connectivity or information access for the Supplier in the following cases:

a) Supplier refuses the Client to conduct a security audit

b) corrective actions are not implemented, or

c) lack of collaboration in case of a major Security Incident.

Supplier shall implement a formal change control process for software and hardware Products.

Supplier Relationships

Supplier shall systematically use malware detection tools before delivery to Client and provide to Client the report of this malware detection.

Information Security Incident management

The Supplier shall implement a comprehensive and approved Security Incident management process for information and systems it operates, that includes identification, response, containment, recovery, reporting, evidence protection and post-implementation review of information Security Incidents.

The Supplier agrees to notify Thales CERT without undue delay, and in any event no later than 24 hours, upon learning of Security Incidents at the following address: CERT@thalesgroup.com. The notification shall include at least:
a) problem statemen t or description
b) expected resolution time (if known),
c) and the name and phone number of the Supplier representative that Client may contact to obtain updates.
Evidence relating to a Security Incident shall be collected, retained and presented by the Supplier to conform to the rules for evidence laid down in the relevant jurisdiction(s).

Compliance

Evidence shall be kept and protected by the Supplier to prove compliance with contractual or applicable legal obligations and made available and delivered where necessary to Client.

Operations Security

The Supplier shall maintain a security environment designed to ensure that the Products are protected from malware. In particular, the Supplier shall:

a) use all care and means available to prevent intrusion of malicious code on its servers, workstations and all possible infrastructure (e.g. e-mail gateways, etc.);

b) implement detection, prevention and recovery controls to protect against malware for its systems. Applicable quarantine measures shall be enforced on infected network devices until they are cleaned;

c) ensure that anti-virus/anti-intrusion software engines, and their patterns/signatures databases, are updated regularly on all devices, including mobile ones.

The Supplier agrees to provide applicable and necessary security patches to all systems and software that process, store or otherwise support the Products, including, operating system, open source, and application software, and the like, as quickly as reasonably possible during all their lifecycle.

Information security aspects of business continuity management

The Supplier shall have deployed the means to ensure business continuity and recovery in case of a disaster, including resilience of the Products delivered to Client.

The Supplier shall notify Client when a disaster occurs.

SECURITY REQUIREMENTS - SOFTWARE

Definition

Security Incident: a breach of security leading to a successful or an imminent threat of (i) unauthorized or unlawful access, use, disclosure, modification, theft, loss, corruption/alteration or destruction of data belonging to Client (or the Client's customer) (ii) interference with information technology operations, or (iii) interference with system operations.

Organisation of information security

Before the delivery of the Products, the Supplier shall communicate to Client its governance regarding security and cybersecurity including points of contact and their responsibilities and tasks.

System acquisition, development and maintenance

Information about technical vulnerabilities of information systems or components being used by the Supplier to provide the Products shall be communicated to the Client in a timely fashion, the Client's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

The Supplier shall ensure an annual basis review and audit of its systems' security robustness. To do so, the Supplier will conduct periodic reviews of the security of its network and adequacy of its information security program as measured against applicable industry security standards and its policies and procedures. The Supplier will continually evaluate the security of its network and associated services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.

The Supplier shall identify, initiate, manage, record, report and close down all appropriate remedial/corrective actions in respect of any defects identified by any security audit, review, monitoring activity or incident, in a timeframe commensurate with the impact of the defect and the required implementation workload.

Client reserves the right to discontinue or restrict the connectivity or information access for the Supplier in the following cases:

a) Supplier refuses the Client to conduct a security audit

b) corrective actions are not implemented, or

c) lack of collaboration in case of a major Security Incident.

Supplier shall implement a formal change control process for software and hardware Products.

Supplier Relationships

Supplier shall systematically use malware detection tools before delivery to Client and provide to Client the report of this malware detection.

Information Security Incident management

The Supplier shall implement a comprehensive and approved Security Incident management process for information and systems it operates, that includes identification, response, containment, recovery, reporting, evidence protection and post-implementation review of information Security Incidents.

The Supplier agrees to notify Thales CERT without undue delay, and in any event no later than 24 hours, upon learning of Security Incidents at the following address: CERT@thalesgroup.com. The notification shall include at least:
a) problem statemen t or description
b) expected resolution time (if known),
c) and the name and phone number of the Supplier representative that Client may contact to obtain updates.
Evidence relating to a Security Incident shall be collected, retained and presented by the Supplier to conform to the rules for evidence laid down in the relevant jurisdiction(s).

Compliance

Evidence shall be kept and protected by the Supplier to prove compliance with contractual or applicable legal obligations and made available and delivered where necessary to Client.

Operations Security

The Supplier shall maintain a security environment designed to ensure that the Products are protected from malware. In particular, the Supplier shall:

a) use all care and means available to prevent intrusion of malicious code on its servers, workstations and all possible infrastructure (e.g. e-mail gateways, etc.);

b) implement detection, prevention and recovery controls to protect against malware for its systems. Applicable quarantine measures shall be enforced on infected network devices until they are cleaned;

c) ensure that anti-virus/anti-intrusion software engines, and their patterns/signatures databases, are updated regularly on all devices, including mobile ones.

The Supplier agrees to provide applicable and necessary security patches to all systems and software that process, store or otherwise support the Products, including, operating system, open source, and application software, and the like, as quickly as reasonably possible during all their lifecycle.

Information security aspects of business continuity management

The Supplier shall have deployed the means to ensure business continuity and recovery in case of a disaster, including resilience of the Products delivered to Client.

The Supplier shall notify Client when a disaster occurs.

SECURITY REQUIREMENTS - BUILD TO PRINT / BUILD TO SPECIFICATIONS HARDWARE

Definitions

Thales Asset: (i) any non-tangible asset of the Client, such as files, data received and processed and deleted and/or data of the Client, which is used for the performance of the Services, and/or (ii) any tangible asset of the Client which is used, transformed or/and transferred in the context of the Services.

Security Incident: a breach of security leading to a successful or an imminent threat of (i) unauthorized or unlawful access, use, disclosure, modification, theft, loss, corruption/alteration or destruction of data belonging to Client (or the Client's customer) (ii) interference with information technology operations, or (iii) interference with system operations.

Information security policies

The Supplier ensures that it has developed and implemented, and will maintain and monitor, a written and comprehensive information security policy (the "security policies") which includes in its scope the sites, activities, personnel and systems used to develop or deliver the Services (e.g. ISO 27001, NIST). The security policies shall define:

- For an organization, the constraints on behavior of its members as well as constraints imposed by mechanisms such as doors, locks, keys and walls.
- For systems, the constraints on functions and flow among them; constraints on access by external systems including programs and access to data by people.

The Supplier shall notify Client within one month any update of its security policies. In any event, the Supplier shall not decrease the security level of the Product or Services. Client may review relevant security policies and procedures at Supplier's site. The Supplier shall comply with the latest version of the Thales Protection of Group Information as communicated by Purchase, which is applicable to the services, products and IT technologies delivered in the course of and for the purpose of the performance of the Services or the delivery of the Products.

Organisation of information security

Before the performance of the Services, the Supplier shall communicate to Client its governance regarding security and cybersecurity including points of contact and their responsibilities and tasks.

Access Control

The Supplier's assigned administrator(s) must retain sole responsibility for granting access to Thales Asset and to Thales Personal Data for all Supplier employees and other users, and for providing a process by which employee and other user accounts shall be created and deleted in a secure and timely fashion. This process must include appropriate leadership approval, auditable history of all changes, and an annual review of access authorization and excess access remediation.

The Supplier shall establish, maintain and enforce the security access principles of "segregation of duties" and "dual control" and "least privilege" with respect to Thales Asset and Thales Personal Data.

The Supplier shall register and keep the logs to any access to Thales Assets, Thales Personal Data and Thales information system by its staff, agents or sub-contractors, and that these logs shall be communicated to Client.

Asset / Thales Personal Data management

The Supplier shall establish and maintain administrative, technical and physical safeguards to protect the security, integrity, confidentiality and availability of Thales Asset and Thales Personal Data and, including to protect Thales Asset and Thales Personal Data against any anticipated threats, hazards, and to protect against any Security Incident.

The Supplier maintains an inventory of all Thales Assets (or of the components that support those Assets).

Physical and environmental security

The Supplier shall comply with the Prevention Plan communicated by Client and which is applicable to the Services and IT technologies delivered in the course of and for the purpose of the Services.

Operations security

The Supplier shall maintain a security environment designed to ensure that the Services are protected from malware. In particular, the Supplier shall:
a) use all care and means available to prevent intrusion of malicious code on its servers, workstations and all possible infrastructure (e.g. e-mail gateways, etc.);
b) implement detection, prevention and recovery controls to protect against malware for its systems. Applicable quarantine measures shall be enforced on infected network devices until they are cleaned;
c) ensure that anti-virus/anti-intrusion software engines, and their patterns/signatures databases, are updated regularly on all devices, including mobile ones.

The Supplier shall ensure that critical patches are applied to its systems as recommended by software vendors, and after being tested by the Supplier for compatibility with its installations.
Supplier agrees to maintain and enforce retention policies for any and all reports, logs, audit trails and any other documentation that provides evidence of security, systems, and audit processes and procedures according to requirements mutually agreed upon by Thales and Supplier, one (1) year being Thales's standard retention requirement. Such retention period may change in accordance with all applicable laws and regulations.

The Supplier agrees to employ supported software (e.g., software under active maintenance, including operating system, open source, application software and/or the like) on any systems that process, store or otherwise support the Services. The Supplier shall notify Client in advance (1 year) of any end of support of any component.

System acquisition, development and maintenance

Rules for the development of software and systems shall be established and applied to developments within the organization. At least, rules for software development shall include:
a) No hardcoded credentials shall be used
b) Administrator and user roles shall be separated
c) All default accounts used in the development process shall systematically be removed and the default password shall be changed before delivery to Client.

Supplier shall provide evidences of the following points concerning the design of its Services:
a) Cyber risks faced by the Services shall be identified and lead to the creation of appropriate cybersecurity controls to be put in place.
b) Trusted and untrusted data sources (for example, data sources internal to the Client's organization

could be considered as trusted whereas other data sources might be considered as untrusted) shall be identified.

The Supplier agrees to perform (at least annually) a vulnerability threat assessment test or such other testing of its systems that have access to or contain Thales Asset and Thales Personal Data and shall mitigate or remediate critical findings in a timeframe commensurate with the impact of the defect and the required implementation workload. Upon request, the Supplier agrees to provide Client with reports which may include a date of the test, who performed the test, and an indication of the relative risk of identified vulnerabilities, as well as a timeline to remediate any findings. The vulnerability threat assessment shall be performed using industry standard threat assessment tools and or services. The Supplier shall ensure an annual basis review and audit of its systems' security robustness. To do so, the Supplier will conduct periodic reviews of the security of its network and adequacy of its information security program as measured against applicable industry security standards and its policies and procedures.The Supplier will continually evaluate the security of its network and associated services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews. The Supplier shall identify, initiate, manage, record, report and close down all appropriate remedial/corrective actions in respect of any defects identified by any security audit, review, monitoring activity or incident, in a timeframe commensurate with the impact of the defect and the required implementation workload. Client reserves the right to discontinue or restrict the connectivity or information access for the Supplier in the following cases:
a) Supplier refuses the Client to conduct a security audit
b) corrective actions are not implemented, or
c) lack of collaboration in case of a major Security Incident. Supplier shall implement a formal change control process for software and hardware Products. Information about technical vulnerabilities of information systems or components being used by the Supplier to provide the Services shall be communicated to the Client in a timely fashion, the Client's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

Supplier Relationships

The Supplier shall systematically use malware detection tools before delivery to Client and provide to Client the report of this malware detection.

Information Security Incident management

The Supplier shall implement a comprehensive and approved Security Incident management process for information and systems it operates, that includes identification, response, containment, recovery, reporting, evidence protection and post-implementation review of information Security Incidents.

The Supplier agrees to notify Thales CERT without undue delay, and in any event no later than 24 hours, upon learning of Security Incidents at the following address: CERT@thalesgroup.com. The notification shall include at least:
a) problem statemen t or description
b) expected resolution time (if known),
c) and the name and phone number of the Supplier representative that Client may contact to obtain updates.
Evidence relating to a Security Incident shall be collected, retained and presented by the Supplier to conform to the rules for evidence laid down in the relevant jurisdiction(s).

Information security aspects of business continuity management

The Supplier shall have deployed the means to ensure business continuity and recovery in case of a disaster, including resilience of the Products or Services delivered to Client. The Supplier shall notify Client when a disaster occurs.

Compliance

The Supplier acknowledges that Client or an independent auditor designated by Client, at its own expense, may audit and monitor to confirm the compliance with the security agreements of systems, processes and procedures of the Supplier and its supply chain, relevant to the Services provided to Client or where Client systems or information may be placed or accessed from. This includes but is not limited to verifying information access approval and control, control of information flow, and audit trails. The Supplier will provide all relevant documentation and evidence. Due to the confidential and proprietary nature of the Supplier's operations, and in order to protect the integrity and security of the Supplier's operations and the shared nature of systems which may be used to provide the Services under the Order:
a) both Parties shall agree in advance the scope of such inspections,
b) a written notice of no less than 30 days prior to the anticipated start date of the inspection shall be given by the Client and may occur no more than once in any twelve (12)-month period, barring exigent circumstances, such as Client's reasonable concern of a Security Incident, in which case an inspection may be performed in response to such circumstance or concern, and at a time mutually agreed by both Parties.
c) if to be conducted by a third party, the third party must be a mutually agreed upon security assessment specialist, where such agreement by Supplier shall not be unreasonably withheld,
d) are subject to appropriate confidentiality and non-disclosure provisions, and
e) may not unreasonably disrupt Supplier normal business or IT operations.

Notwithstanding the foregoing, the Client retains the sole discretion as to whether to initiate a security review under this section, and may initiate such a review prior to production use of the Services and thereafter, (2) upon any change in the Services that could affect the security of any element thereof, (3) following any Security Incident affecting the Products or Services or Thales Assets or Thales Personal Data, and (4) upon Client's request or demand from a governmental body having jurisdiction. The Supplier shall provide Client with reasonable assistance as may be required to enable Client to comply with applicable laws in connection with any issues implicated by a security review.Evidence shall be kept and protected by the Supplier to prove compliance with contractual or applicable legal obligations and made available and delivered where necessary to Client.

SECURITY REQUIREMENTS - SAAS

Definitions

Thales Asset: (i) any non-tangible asset of the Client, such as files, data received and processed and deleted and/or data of the Client, which is used for the performance of the Services, and/or (ii) any tangible asset of the Client which is used, transformed or/and transferred in the context of the Services.

Security Incident: a breach of security leading to a successful or an imminent threat of (i) unauthorized or unlawful access, use, disclosure, modification, theft, loss, corruption/alteration or destruction of data belonging to Client (or the Client's customer) (ii) interference with information technology operations, or (iii) interference with system operations.

Information security policies

The Supplier ensures that it has developed and implemented, and will maintain and monitor, a written and comprehensive information security policy (the "security policies") which includes in its scope the sites, activities, personnel and systems used to develop or deliver the Services (e.g. ISO 27001, NIST). The security policies shall define:

- For an organization, the constraints on behavior of its members as well as constraints imposed by mechanisms such as doors, locks, keys and walls.
- For systems, the constraints on functions and flow among them; constraints on access by external systems including programs and access to data by people.

The Supplier shall notify Client within one month any update of its security policies. In any event, the Supplier shall not decrease the security level of the Product or Services. Client may review relevant security policies and procedures at Supplier's site. The Supplier shall comply with the latest version of the Thales Protection of Group Information as communicated by Purchase, which is applicable to the services, products and IT technologies delivered in the course of and for the purpose of the performance of the Services or the delivery of the Products.

Organisation of information security

Before the performance of the Services, the Supplier shall communicate to Client its governance regarding security and cybersecurity including points of contact and their responsibilities and tasks.

Access Control

The Supplier's assigned administrator(s) must retain sole responsibility for granting access to Thales Asset and to Thales Personal Data for all Supplier employees and other users, and for providing a process by which employee and other user accounts shall be created and deleted in a secure and timely fashion. This process must include appropriate leadership approval, auditable history of all changes, and an annual review of access authorization and excess access remediation.

The Supplier shall establish, maintain and enforce the security access principles of "segregation of duties" and "dual control" and "least privilege" with respect to Thales Asset and Thales Personal Data.

The Supplier shall register and keep the logs to any access to Thales Assets, Thales Personal Data and Thales information system by its staff, agents or sub-contractors, and that these logs shall be communicated to Client.

Asset / Thales Personal Data management

The Supplier shall establish and maintain administrative, technical and physical safeguards to protect the security, integrity, confidentiality and availability of Thales Asset and Thales Personal Data and, including to protect Thales Asset and Thales Personal Data against any anticipated threats, hazards, and to protect against any Security Incident.

Physical and environmental security

The Supplier shall provide the geographic locations in which it operates Thales Assets and/or processes Thales personal data. In particular, the Supplier shall provide the address of its
a) Primary Data Centre and / or computer facility and
b) Backup and / or Disaster Recover Site.

Operations security

The Supplier shall maintain a security environment designed to ensure that the Services are protected from malware. In particular, the Supplier shall:
a) use all care and means available to prevent intrusion of malicious code on its servers, workstations and all possible infrastructure (e.g. e-mail gateways, etc.);
b) implement detection, prevention and recovery controls to protect against malware for its systems. Applicable quarantine measures shall be enforced on infected network devices until they are cleaned;
c) ensure that anti-virus/anti-intrusion software engines, and their patterns/signatures databases, are updated regularly on all devices, including mobile ones.

The Supplier shall ensure that critical patches are applied to its systems as recommended by software vendors, and after being tested by the Supplier for compatibility with its installations.
Supplier agrees to maintain and enforce retention policies for any and all reports, logs, audit trails and any other documentation that provides evidence of security, systems, and audit processes and procedures according to requirements mutually agreed upon by Thales and Supplier, one (1) year being Thales's standard retention requirement. Such retention period may change in accordance with all applicable laws and regulations.

The Supplier agrees to employ supported software (e.g., software under active maintenance, including operating system, open source, application software and/or the like) on any systems that process, store or otherwise support the Services. The Supplier shall notify Client in advance (1 year) of any end of support of any component.

The Supplier shall explain its multi-tenant policy and shall particularly detail how tenant's isolation is performed.

System acquisition, development and maintenance

Rules for the development of software and systems shall be established and applied to developments within the organization. At least, rules for software development shall include:
a) No hardcoded credentials shall be used
b) Administrator and user roles shall be separated
c) All default accounts used in the development process shall systematically be removed and the default password shall be changed before delivery to Client.

Supplier shall provide evidences of the following points concerning the design of its Services:
a) Cyber risks faced by the Services shall be identified and lead to the creation of appropriate cybersecurity controls to be put in place.
b) Trusted and untrusted data sources (for example, data sources internal to the Client's organization

could be considered as trusted whereas other data sources might be considered as untrusted) shall be identified.

The Supplier agrees to perform (at least annually) a vulnerability threat assessment test or such other testing of its systems that have access to or contain Thales Asset and Thales Personal Data and shall mitigate or remediate critical findings in a timeframe commensurate with the impact of the defect and the required implementation workload. Upon request, the Supplier agrees to provide Client with reports which may include a date of the test, who performed the test, and an indication of the relative risk of identified vulnerabilities, as well as a timeline to remediate any findings. The vulnerability threat assessment shall be performed using industry standard threat assessment tools and or services. The Supplier shall ensure an annual basis review and audit of its systems' security robustness. To do so, the Supplier will conduct periodic reviews of the security of its network and adequacy of its information security program as measured against applicable industry security standards and its policies and procedures.The Supplier will continually evaluate the security of its network and associated services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews. The Supplier shall identify, initiate, manage, record, report and close down all appropriate remedial/corrective actions in respect of any defects identified by any security audit, review, monitoring activity or incident, in a timeframe commensurate with the impact of the defect and the required implementation workload. Client reserves the right to discontinue or restrict the connectivity or information access for the Supplier in the following cases:
a) Supplier refuses the Client to conduct a security audit
b) corrective actions are not implemented, or
c) lack of collaboration in case of a major Security Incident. Supplier shall implement a formal change control process for software and hardware Products. Information about technical vulnerabilities of information systems or components being used by the Supplier to provide the Services shall be communicated to the Client in a timely fashion, the Client's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

Supplier Relationships

The Supplier shall systematically use malware detection tools before delivery to Client and provide to Client the report of this malware detection.

Information Security Incident management

The Supplier shall implement a comprehensive and approved Security Incident management process for information and systems it operates, that includes identification, response, containment, recovery, reporting, evidence protection and post-implementation review of information Security Incidents.

The Supplier agrees to notify Thales CERT without undue delay, and in any event no later than 24 hours, upon learning of Security Incidents at the following address: CERT@thalesgroup.com. The notification shall include at least:
a) problem statemen t or description
b) expected resolution time (if known),
c) and the name and phone number of the Supplier representative that Client may contact to obtain updates.
Evidence relating to a Security Incident shall be collected, retained and presented by the Supplier to conform to the rules for evidence laid down in the relevant jurisdiction(s).

Information security aspects of business continuity management

The Supplier shall have deployed the means to ensure business continuity and recovery in case of a disaster, including resilience of the Products or Services delivered to Client. The Supplier shall notify Client when a disaster occurs.

Compliance

The Supplier acknowledges that Client or an independent auditor designated by Client, at its own expense, may audit and monitor to confirm the compliance with the security agreements of systems, processes and procedures of the Supplier and its supply chain, relevant to the Services provided to Client or where Client systems or information may be placed or accessed from. This includes but is not limited to verifying information access approval and control, control of information flow, and audit trails. The Supplier will provide all relevant documentation and evidence. Due to the confidential and proprietary nature of the Supplier's operations, and in order to protect the integrity and security of the Supplier's operations and the shared nature of systems which may be used to provide the Services under the Order:
a) both Parties shall agree in advance the scope of such inspections,
b) a written notice of no less than 30 days prior to the anticipated start date of the inspection shall be given by the Client and may occur no more than once in any twelve (12)-month period, barring exigent circumstances, such as Client's reasonable concern of a Security Incident, in which case an inspection may be performed in response to such circumstance or concern, and at a time mutually agreed by both Parties.
c) if to be conducted by a third party, the third party must be a mutually agreed upon security assessment specialist, where such agreement by Supplier shall not be unreasonably withheld,
d) are subject to appropriate confidentiality and non-disclosure provisions, and
e) may not unreasonably disrupt Supplier normal business or IT operations.

Notwithstanding the foregoing, the Client retains the sole discretion as to whether to initiate a security review under this section, and may initiate such a review prior to production use of the Services and thereafter, (2) upon any change in the Services that could affect the security of any element thereof, (3) following any Security Incident affecting the Products or Services or Thales Assets or Thales Personal Data, and (4) upon Client's request or demand from a governmental body having jurisdiction. The Supplier shall provide Client with reasonable assistance as may be required to enable Client to comply with applicable laws in connection with any issues implicated by a security review.Evidence shall be kept and protected by the Supplier to prove compliance with contractual or applicable legal obligations and made available and delivered where necessary to Client. The Supplier shall promptly notify Client upon the receipt of any request requiring that Client Data/Thales Asset be supplied to any other third party, including public administrations or authorities. The Supplier shall use all legal means to contest such access requests unless approved by Client.

The Supplier shall be certified according to ISO 27001 standard.