Security requirements - Service provision

Definitions

EPSA MARKETPLACE Property: any (i) logical element, in particular files, data received, processed and deleted and/or Customer data (with the exception of the Customer's Personal Data) incorporated into the Services or (ii) tangible property belonging to the Customer (including deliverables) used, transformed and/or transferred for the performance of the Services.

Security Incident: a breach of security that results in a real or imminent threat of unauthorised or unlawful access, use, disclosure, infringement, modification, theft, loss, corruption/alteration or destruction of EPSA MARKETPLACE Property/Customer Personal Data; interference with computer operations or interference with the functioning of the system. This covers, in particular, loss or theft of mobile devices, malfunctions, power failure, overloads, errors made by users/IT system staff, access violations, malware and hacking.

Security Policy: the security requirements for a system and/or an organisation.

- For an organisation, physical security requirements such as doors, locks, keys and walls;
- For systems, the constraints imposed on functions and the flows between them, and the constraints imposed on access by external systems, particularly programs, and on access to data by individuals.

On-site services: Services provided by a Supplier working on a Customer's site or on the site of the Customer's own customer and accessing the information system of the Customer or their customer.

Off-site services connected to the Customer's information system: Services provided from the site of the Supplier, accessing the information system of the Customer or their customer:

- in a dedicated, secure area reserved for Customers only;
- or from their premises, in compliance with EPSA MARKETPLACE security rules.

Off-site services not connected to the Customer's IT system: Services provided from the site of the Supplier, without accessing the information system of the Customer or their customer:

Security Policy

The Supplier warrants that it has developed, implemented and will maintain and monitor a comprehensive written Security Policy containing security requirements for the sites, activities, personnel and systems used to develop, perform and deliver the Services (e.g. ISO 27001, NIST).

In the case of Services performed off-site (whether connected to the Customer's information system or not):

a. The Supplier shall notify the Customer within one (1) month of any update to its Security Policy. In any event, the Supplier shall not reduce the level of security of the Services.

b. The Customer may review the security policies and procedures on the Supplier's site which may affect the performance of the Services.

The Supplier shall comply with the latest version of EPSA MARKETPLACE's Information Protection as communicated by the Customer, applicable to the products, services and computer technologies delivered as part of the performance of the Services or necessary for the performance of the Services.

Organisation of information security

Prior to the performance of the Services, the Supplier shall communicate to the Customer its governance rules concerning security and cybersecurity, including the points of contact and their responsibilities and tasks.

Human Resources Security

When the Supplier carries out work on the site of the Customer or their customer, it shall comply with the internal physical and logical security rules and regulations applicable to such sites, and acknowledges its responsibilities with regard to security and the consequences of non-compliance with security rules.

Management of EPSA MARKETPLACE Property/Customer Personal Data

In the case of Services performed off-site (whether connected to the Customer's information system or not):

a. The Supplier shall establish and maintain administrative, technical and physical safeguards to protect the security, integrity, confidentiality and availability of EPSA MARKETPLACE's Property and the Customer's Personal Data and, in particular, to protect EPSA MARKETPLACE's Property and the Customer's Personal Data against any threats or anticipated danger and to protect them against Security Incidents.

b. The Supplier shall maintain an inventory of all EPSA MARKETPLACE Property (or components supporting such Property).

Access Control

In the case of Services performed off-site (whether connected to the Customer's information system or not):

a. The Supplier's administrators assume full responsibility for granting access to EPSA MARKETPLACE Property and Customer Personal Data to all of the Supplier's employees and other users, and for providing a process that will manage the secure and timely creation and deletion of employee and other user accounts. This process must include appropriate management approval, a verifiable history of all changes and an annual review of access authorisation and remediation of excessive access. The Supplier shall establish, maintain and apply the security access principles of "Segregation of Duties", "Dual Control" and "Least Privilege" in relation to EPSA MARKETPLACE Property and the Customer's Personal Data.

b. The Supplier will record and keep logs of all accesses to EPSA MARKETPLACE's Property, the Customer's Personal Data and the Customer's information system by its staff, agents or subcontractors and these logs will be communicated to the Customer. In the case of Services performed off Customer site connected to EPSA MARKETPLACE's information system, the Supplier shall submit to the Customer for approval the identity of any employee of the Supplier who will be granted remote access privileges to the Customer's information

systems and networks hosted on the Customer's site. This applies in particular when the operation involves creating an account for a person in the Customer's directory.

Physical and environmental safety

If the Supplier provides Services to the Customer from its premises, it will comply with the Prevention Plan communicated by the Customer insofar as it is applicable to the services and computer technologies delivered as part of the performance of the Services or necessary for the performance of the Services. In the case of Services carried out off Customer site connected to EPSA MARKETPLACE's information system, the Supplier will indicate the geographical locations in which it operates EPSA MARKETPLACE's Property and/or processes the Customer's Personal Data. In particular, the Supplier shall provide the address of their:

a. primary data centre and/or IT facility and,

b. backup and/or disaster recovery site.

Security of operations

The Supplier will maintain a security environment designed to ensure that the Services are protected against malicious code. In particular, the Supplier will:

a. take all precautions and use all available means to prevent the intrusion of malicious code on its servers, workstations and any infrastructure (e.g. e-mail gateway, etc.);

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

c. ensure that anti-virus/anti-intrusion software engines and their signature templates/databases are regularly updated on all devices, including mobile devices. The Supplier shall ensure that critical patches are applied to its systems in accordance with software suppliers' recommendations and after the Supplier has tested their compatibility with its installations. In the case of Services performed off-site (whether connected to the Customer's information system or not):

a. The Supplier undertakes to use commercially supported software (e.g. software under active maintenance, including operating system, open source or application software and/or similar) on any systems that process, store or technically support the Services.

b. The Supplier shall notify the Customer one (1) year prior to the termination of commercial support for any component.

Systems acquisition, development and maintenance

Rules for the development of software and systems which will be defined and applied to developments within the organisation. In the case of Services performed off-site (whether connected to the Customer's information system or not) the rules for software development will include at least:

a. no use of hard-coded identifiers;

b. separation of administrator and user roles;

c. systematic deletion of all default accounts used in the development process and modification of the default password before delivery to the Customer. The Supplier shall provide evidence on the following points concerning the performance of the Services:

a. the cyber-risks to which the Services are exposed will be identified and will lead to the creation of appropriate cyber-security controls to be put in place;

b. reliable and unreliable data sources will be identified (for example, data sources internal to the Customer's organisation may be considered reliable, while other data sources may be considered unreliable). The Supplier undertakes to carry out (at least annually) a vulnerability assessment of its systems accessing or containing EPSA MARKETPLACE Property and/or the Customer's personal data and will mitigate risks or remedy critical defects within an appropriate timeframe having regard to the importance of the defect and the workload required for remediation. The Supplier undertakes to provide the Customer with reports specifying the date of the assessment, the identity of the persons who carried out the assessment and an indication of the risk relating to the vulnerabilities identified as well as the time required to remedy them. The vulnerability threat assessment will be carried out using industry-standard tools and/or services. The Supplier will implement a process for controlling technical modifications to software and hardware products.

The Supplier shall systematically use malware detection tools before any deliverable is delivered and shall provide the Customer with a report on the detection of such malware.

In the case of Services performed on the Customer's site:

a. The Supplier will carry out an annual review and check of the reliability of the system security. To this end, the Supplier will carry out periodic reviews of the security of its network and the adequacy of its Security Policy in relation to industry security standards and its procedures. The Supplier will regularly assess the security of its network and associated services in order to determine whether additional or different security measures are required to respond to new security risks or to the conclusions generated by periodic assessments. The Supplier shall identify, initiate, manage, record, report and implement all appropriate remediation/correction measures relating to any defect identified by an audit, assessment, monitoring activity or Security Incident, within an appropriate timeframe having regard to the significance of the defect and the workload required for remediation.

b. The Customer reserves the right to interrupt or limit connectivity or access to the Supplier's information in the following cases:

- the Supplier refuses to allow the Customer to carry out a security audit;
- corrective measures are not put in place; or
- failure to cooperate in the event of a major Security Incident.

Security Incident Management

The Supplier shall put in place a thorough and agreed Security Incident management process for the networks and systems it operates, including the identification, response, containment, recovery, reporting, evidence protection and review of Security Incidents;. The Supplier undertakes to inform the Customer without delay of the occurrence of an event, no later than twenty-four (24) hours after becoming aware of a Security Incident, at the following address: contact@epsa-marketplace.com. The notification must include at least:

a. a statement or description of the problem;

b. the expected remediation period (if known);

c. the name and telephone number of the Supplier's representative whom the Customer may contact to obtain further information. Evidence relating to a Security Incident will be collected, kept and presented by the Supplier in order to comply with the rules of evidence applicable before the competent courts.

Business continuity management

In the case of Services performed off-site (whether connected to the Customer's information system or not):

a. The Supplier will have deployed the means to ensure business continuity and disaster recovery, including the resilience of the Services delivered to the Customer;

b. The Supplier shall notify the Customer in the event of a claim.

Compliance

In the case of Services performed off-site (whether connected to the Customer's information system or not):

a. The Supplier acknowledges that the Customer or an independent auditor appointed by the Customer may, at its own expense, carry out an audit of the Supplier's compliance with its security commitments on its systems, processes and procedures and supply chain, affecting the Customer's Services or systems. This includes, in particular, verifying agreement and access control, controlling the flow of information and audit logs. The Supplier will provide all the necessary documentation and proof.

b. Due to the confidential and exclusive nature of the Supplier's operations, and in order to protect the integrity and security of such operations and the shared nature of the systems that may be used to provide the Services:

- the parties will agree in advance on the scope of the audits;
- at least thirty (30) days' written notice shall be given by the Customer prior to the date on which the audit is due to commence and the audit shall take place no more than once in any twelve (12) month period, unless there are circumstances such as a reasonable suspicion on the part of the Customer of a Security Incident, in which case an audit may be carried out on a date mutually agreed by the parties;
- if the audit is carried out by a third party, the latter shall be an expert auditor in the field of security and approved by the parties, it being understood that the Supplier may not refuse the third party auditor without a legitimate reason;
- the audit will be conducted in accordance with the confidentiality and non-disclosure requirements and constraints of the parties; and
- the audit must not unreasonably disrupt the Supplier's normal business or IT operations.

c. Notwithstanding the above, the Customer retains the discretion to initiate a security inspection under this section, and may initiate the inspection prior to the performance of the Services and thereafter, (i) in the event of any change in the performance of the Services which may affect the security thereof, (ii) following any Security Incident affecting the Services or EPSA MARKETPLACE's Property or the Customer's Personal Data, and (iii) in the event of a request from the Customer or a request from a government agency. The Supplier shall provide the Customer with such reasonable assistance as may be necessary to enable the Customer to comply with applicable security laws.

The Supplier shall keep and protect any proof of compliance with legal or contractual obligations and shall make such proof available to the Customer if necessary

Security requirements - Off-the-shelf products

Definitions

Security Incident: a breach of security that results in a real or imminent threat of unauthorised or unlawful access, use, disclosure, infringement, modification, theft, loss, corruption/alteration or destruction of EPSA MARKETPLACE Property/Customer Personal Data, interference with computer operations or interference with the functioning of the system. This covers, in particular, loss or theft of mobile devices, malfunctions, power failure, overloads, errors made by users/IT system staff, access violations, malware and hacking.

Security Policy: the security requirements for a system and/or an organisation;

- For an organisation, physical security requirements such as doors, locks, keys and walls;
- For systems, the constraints imposed on functions and the flows between them, and the constraints imposed on access by external systems, particularly programs, and on access to data by individuals.

Organisation of information security

Prior to delivery of the Products, the Supplier shall communicate to the Customer its governance rules concerning security and cyber security, including the points of contact and their responsibilities and tasks.

Security of operations

The Supplier shall maintain a security environment designed to ensure that the Products or services associated with the Products are protected against malicious programs. In particular, the Supplier will:

a. take all precautions and use all available means to prevent the intrusion of malicious code on its servers, workstations and any infrastructure (e.g. e-mail gateway, etc.);

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

c. ensure that anti-virus/anti-intrusion software engines and their signature templates/databases are regularly updated on all devices, including mobile devices.

The Supplier shall ensure that critical patches are applied to its systems in accordance with software suppliers' recommendations and after the Supplier has tested their compatibility with its installations.

Systems acquisition, development and maintenance.

The Supplier shall systematically use malware detection tools prior to any delivery of the Product and shall provide the Customer with a report on the detection of such malware.

The Supplier will carry out an annual review and check of the reliability of the system's security. To this end, the Supplier will carry out periodic reviews of the security of its network and the adequacy of its Security Policy in relation to industry security standards and its procedures. The Supplier will regularly assess the security of its network and associated services in order to determine whether additional or different security measures are required to respond to new security risks or to the conclusions generated by periodic assessments. The Supplier shall identify, initiate, manage, record, report and implement all appropriate remediation/correction measures relating to any defect identified by an audit, assessment, monitoring activity or Security Incident, within an appropriate timeframe having regard to the significance of the defect and the workload required for remediation.

The Customer reserves the right to interrupt or limit connectivity or access to the Supplier's information in the following cases:

- the Supplier refuses to allow the Customer to carry out a security audit;
- corrective measures are not put in place; or
- failure to cooperate in the event of a major Security Incident.

The Supplier will implement a process for controlling technical modifications to software and hardware products.

The Supplier shall systematically use malware detection tools prior to delivery to the Customer and shall provide the Customer with the report on the detection of such malware.

Management of information security incidents

The Supplier will implement a thorough and agreed Security Incident Management process for the networks and systems it operates, including the identification, response, containment, recovery, reporting, evidence protection and review of Security Incidents. The Supplier undertakes to inform the Customer without delay of the occurrence of an event, no later than twenty-four (24) hours after becoming aware of a Security Incident, at the following address: Contact@epsa-marketplace.com. The notification must include at least:

a. a statement or description of the problem;

b. the expected remediation period (if known);

c. the name and telephone number of the Supplier's representative whom the Customer may contact to obtain further information.

Evidence relating to a Security Incident will be collected, kept and presented by the Supplier in order to comply with the rules of evidence applicable before the competent courts.

Business continuity management

The Supplier shall have deployed the means to ensure business continuity and disaster recovery, including the resilience of the Products delivered to the Customer. The Supplier shall notify the Customer in the event of a claim

Definitions

EPSA MARKETPLACE Property: any (i) logical element, in particular files, data received, processed and deleted and/or Customer data (with the exception of the Customer's Personal Data) incorporated into the Services or (ii) tangible property belonging to the Customer (including deliverables) used, transformed and/or transferred for the performance of the Services.

Security Incident: a breach of security that results in a real or imminent threat of unauthorised or unlawful access, use, disclosure, infringement, modification, theft, loss, corruption/alteration or destruction of EPSA MARKETPLACE Property/Customer Personal Data, interference with computer operations or interference with the functioning of the system. This covers, in particular, loss or theft of mobile devices, malfunctions, power failure, overloads, errors made by users/IT system staff, access violations, malware and hacking.

Security Policy: the security requirements for a system and/or an organisation;

- for an organisation, physical security requirements such as doors, locks, keys and walls;
- for systems, the constraints imposed on functions and the flows between them, and the constraints imposed on access by external systems, particularly programs, and on access to data by individuals.

Organisation of information security

Prior to delivery of the Products, the Supplier shall communicate to the Customer its governance rules concerning security and cyber security, including the points of contact and their responsibilities and tasks.

Security of operations

The Supplier shall maintain a security environment designed to ensure that the Products or services associated with the Products are protected against malicious programs. In particular, the Supplier will:

a. take all precautions and use all available means to prevent the intrusion of malicious code on its servers, workstations and any infrastructure (e.g. e-mail gateway, etc.);

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

c. ensure that anti-virus/anti-intrusion software engines and their signature templates/databases are regularly updated on all devices, including mobile devices.

The Supplier shall ensure that critical patches are applied to its systems in accordance with software suppliers' recommendations and after the Supplier has tested their compatibility with its installations.

Systems acquisition, development and maintenance

The Supplier shall systematically use malware detection tools prior to any delivery of the Product and shall provide the Customer with a report on the detection of such malware.

The Supplier will carry out an annual review and check of the reliability of the system's security. To this end, the Supplier will carry out periodic reviews of the security of its network and the adequacy of its Security Policy in relation to industry security standards and its procedures. The Supplier will regularly assess the security of its network and associated services in order to determine whether additional or different security measures are required to respond to new security risks or to the conclusions generated by periodic assessments. The Supplier shall identify, initiate, manage, record, report and implement all appropriate remediation/correction measures relating to any defect identified by an audit, assessment, monitoring activity or Security Incident, within an appropriate timeframe having regard to the significance of the defect and the workload required for remediation.

The Customer reserves the right to interrupt or limit connectivity or access to the Supplier's information in the following cases:

- the Supplier refuses to allow the Customer to carry out a security audit;
- corrective measures are not put in place; or
- failure to cooperate in the event of a major Security Incident.

The Supplier will implement a process for controlling technical modifications to software and hardware products.

The Supplier shall systematically use malware detection tools prior to delivery to the Customer and shall provide the Customer with the report on the detection of such malware.

EPSA MARKETPLACE Property Management

The Supplier's service has an automatic deletion facility to delete the Customer's personal data at the end of the data retention period. The Supplier shall, upon request, provide reasonable assistance to the Customer to comply with all laws and regulations applicable to EPSA MARKETPLACE's Property and to personal data relating to, inter alia, identification, labelling, searching, de-identification, signposting, copying, modification, transfer and retrieval. In this case, the Supplier shall provide the Customer with any information they may require or that may prove necessary.

Security Incident Management

The Supplier will implement a thorough and agreed Security Incident Management process for the networks and systems it operates, including the identification, response, containment, recovery, reporting, evidence protection and review of Security Incidents. The Supplier undertakes to inform the Customer without delay of the occurrence of an event, no later than twenty-four (24) hours after becoming aware of a Security Incident, at the following address: Contact@epsa-marketplace.com. The notification must include at least:

a. a statement or description of the problem;

b. the expected remediation period (if known);

c. the name and telephone number of the Supplier's representative whom the Customer may contact to obtain further information. Evidence relating to a Security Incident will be collected, kept and presented by the Supplier in order to comply with the rules of evidence applicable before the competent courts.

Business continuity management

The Supplier shall have deployed the means to ensure business continuity and disaster recovery, including the resilience of the

Products delivered to the Customer. The Supplier shall notify the Customer in the event of a claim.

Definitions

EPSA MARKETPLACE Property: any (i) logical element, in particular files, data received, processed and deleted and/or Customer data (with the exception of the Customer's Personal Data) incorporated into the Services or (ii) tangible property belonging to the Customer (including deliverables) used, transformed and/or transferred for the performance of the Services.

Security Incident: a breach of security that results in a real or imminent threat of unauthorised or unlawful access, use, disclosure, infringement, modification, theft, loss, corruption/alteration or destruction of EPSA MARKETPLACE Property/Customer Personal Data, interference with computer operations or interference with the functioning of the system. This covers, in particular, loss or theft of mobile devices, malfunctions, power failure, overloads, errors made by users/IT system staff, access violations, malware and hacking.

Security Policy: the security requirements for a system and/or an organisation;

- for an organisation, physical security requirements such as doors, locks, keys and walls;
- for systems, the constraints imposed on functions and the flows between them, and the constraints imposed on access by external systems, particularly programs, and on access to data by individuals.

Security Policy

The Supplier warrants that it has developed, implemented, will maintain and monitor a comprehensive written Security Policy containing security requirements for the sites, activities, personnel and systems used to develop, produce and deliver the Products (e.g. ISO 27001, NIST).

The Supplier shall notify the Customer within one (1) month of any update to its Security Policy. In any event, the Supplier shall not reduce the level of security of the Products. The Customer may review the security policies and procedures on the Supplier's site, which may affect the supply of the Products.

The Supplier shall comply with the latest version of the EPSA MARKETPLACE Group's Information Protection as communicated by the Customer, applicable to the products, services and IT technologies necessary for the production and delivery of the Products.

Organisation of information security

Prior to delivery of the Products, the Supplier shall communicate to the Customer its governance rules concerning security and cyber security, including the points of contact and their responsibilities and tasks.

Security of operations

The Supplier will maintain a security environment designed to ensure that the Products are protected against malicious code. In particular, the Supplier will:

a. take all precautions and use all available means to prevent the intrusion of malicious code on its servers, workstations and any infrastructure (e.g. e-mail gateway, etc.);

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

c. ensure that anti-virus/anti-intrusion software engines and their signature templates/databases are regularly updated on all devices, including mobile devices.

The Supplier undertakes to use commercially supported software (e.g. software under active maintenance, including operating system, open source or application software and/or similar) on any systems that process, store or technically support the Services. The Supplier shall notify the Customer one (1) year prior to the termination of commercial support for any component. The Supplier shall ensure that critical patches are applied to its systems in accordance with software suppliers' recommendations and after the Supplier has tested their compatibility with its installations.

The Supplier undertakes to use commercially supported software (e.g. software under active maintenance, including operating system, open source or application software and/or the like) on all systems that technically process, store or support the manufacture of the Products.

The Supplier shall notify the Customer one (1) year in advance of termination of commercial support for any component.

Management of EPSA MARKETPLACE Property/Customer Personal Data

EPSA MARKETPLACE's Property remain the exclusive property of the Customer at all times. The Customer reserves the right to ask the Supplier to diligently amend, update, destroy or return, regardless of the manner, any Customer Property for which the Supplier is responsible. The Supplier shall be able, at the Customer's request, to return and/or delete the Customer's Personal Data no later than one (1) month after the Customer's request.

The Supplier shall establish and maintain administrative, technical and physical safeguards to protect the security, integrity, confidentiality and availability of EPSA MARKETPLACE's Property and the Customer's Personal Data and, in particular, to protect EPSA MARKETPLACE's Property and the Customer's Personal Data against any threats or anticipated danger and to protect them against Security Incidents. The Supplier shall maintain an inventory of all EPSA MARKETPLACE Property (or components supporting such Property).

The Customer Property or any part thereof shall not be retained in any manner whatsoever beyond the period of delivery of Products, except as required by law or by the Customer.

If the Supplier wishes to substantially change the process, method or means of using, disclosing, storing, processing or transmitting or managing EPSA MARKETPLACE Property, the Supplier shall give the Customer at least ninety (90) days' written notice. The Customer shall be entitled, at its sole discretion, to determine whether the changes represent unacceptable risks and may prohibit the Supplier from implementing any such changes to the Products until such time as the risks can be mitigated or an alternative source can be found for the Products.

The Supplier's service has an automatic deletion facility to delete the Customer's Personal Data at the end of the data retention period.

The Supplier shall, upon request, provide reasonable assistance to the Customer to comply with all laws and regulations applicable to EPSA MARKETPLACE's Property and the Customer's Personal Data relating

to, inter alia, identification, labelling, searching, de-identification, signposting, copying, modification, transfer and retrieval. In this case, the Supplier shall provide the Customer with any information they may require or that may prove necessary.

Access control

The Supplier's administrators assume full responsibility for granting access to EPSA MARKETPLACE Property and Customer Personal Data to all of the Supplier's employees and other users, and for providing a process that will manage the secure and timely creation and deletion of employee and other user accounts. This process must include appropriate management approval, a verifiable history of all changes and an annual review of access authorisation and remediation of excessive access. The Supplier shall establish, maintain and apply the security access principles of "Segregation of Duties", "Dual Control" and "Least Privilege" in relation to EPSA MARKETPLACE Property and the Customer's Personal Data.

The Supplier will record and keep logs of all accesses to EPSA MARKETPLACE's Property, the Customer's Personal Data and the Customer's information system by its staff, agents or subcontractors and these logs will be communicated to the Customer.

Systems acquisition, development and maintenance

The Supplier shall systematically use malware detection tools before any deliverable is delivered and shall provide the Customer with a report on the detection of such malware.

The rules for software development will include as a minimum:

a. no use of hard-coded identifiers;

b. separation of administrator and user roles;

c. systematic deletion of all default accounts used in the development process and modification of the default password before delivery to the Customer. The Supplier will provide evidence on the following points concerning the design of the Products: a. the cyber risks faced by the Products will be identified and will lead to the creation of appropriate cyber security controls to be put in place;

d. reliable and unreliable data sources will be identified (for example, data sources internal to the Customer's organisation may be considered reliable while other data sources may be considered unreliable).

The Supplier undertakes to carry out (at least annually) a vulnerability assessment of its systems accessing or containing EPSA MARKETPLACE Property and/or the Customer's personal data and will mitigate risks or remedy critical defects within an appropriate timeframe having regard to the importance of the defect and the workload required for remediation. The Supplier undertakes to provide the Customer with reports specifying the date of the assessment, the identity of the persons who carried out the assessment and an indication of the risk relating to the vulnerabilities identified as well as the time required to remedy them. The vulnerability threat assessment will be carried out using industry-standard tools and/or services.

The Supplier will implement a process for controlling technical modifications to software and hardware products.

Business continuity management

The Supplier shall have deployed the means to ensure business continuity and disaster recovery, including the resilience of the Products delivered to the Customer. The Supplier shall notify the Customer in the event of a claim.

Security Incident Management

The Supplier will implement a thorough and agreed Security Incident Management process for the networks and systems it operates, including the identification, response, containment, recovery, reporting, evidence protection and review of Security Incidents. The Supplier undertakes to inform the Customer without delay of the occurrence of an event, no later than twenty-four (24) hours after becoming aware of a Security Incident, at the following address: Contact@epsa-marketplace.com. The notification must include at least:

a. a statement or description of the problem;

b. the expected remediation period (if known);

c. the name and telephone number of the Supplier's representative whom the Customer may contact to obtain further information.

Evidence relating to a Security Incident will be collected, kept and presented by the Supplier in order to comply with the rules of evidence applicable before the competent courts.

Compliance

The Supplier acknowledges that the Customer or an independent auditor appointed by the Customer may, at its own expense, carry out an audit of the Supplier's compliance with its security commitments on its systems, processes and procedures and supply chain, affecting the Customer's Products or systems. This includes, in particular, verifying agreement and access control, controlling the flow of information and audit logs. The Supplier will provide all the necessary documentation and proof.
Due to the confidential and exclusive nature of the Supplier's operations, and in order to protect the integrity and security of such operations and the shared nature of the systems that may be used to provide the Products:

- the parties will agree in advance on the scope of the audits;
- at least thirty (30) days' written notice shall be given by the Customer prior to the date on which the audit is due to commence and the audit shall take place no more than once in any twelve (12) month period, unless there are circumstances such as a reasonable suspicion on the part of the Customer of a Security Incident, in which case an audit may be carried out on a date mutually agreed by the parties;
- if the audit is carried out by a third party, the latter shall be an expert auditor in the field of security and approved by the parties, it being understood that the Supplier may not refuse the third party auditor without a legitimate reason;
- the audit will be conducted in accordance with the confidentiality and non-disclosure requirements and constraints of the parties; and
- the audit must not unreasonably disrupt the Supplier's normal business or IT operations.

Notwithstanding the provisions above, the Customer retains the discretion to initiate a security inspection under this section, and may initiate the inspection prior to the delivery of Products and thereafter, (i)

in the event of any change in the delivery of the Products which may affect the security thereof, (ii) following any Security Incident affecting the Services or EPSA MARKETPLACE's Property or the Customer's Personal Data, and (iii) in the event of a request from the Customer or a request from a government agency. The Supplier shall provide the Customer with such reasonable assistance as may be necessary to enable the Customer to comply with applicable security laws.

Security requirements - SAAS

Definitions

EPSA MARKETPLACE Property: any (i) logical element, in particular files, data received, processed and deleted and/or Customer data (with

the exception of the Customer's Personal Data) incorporated into the Services or (ii) tangible property belonging to the Customer (including deliverables) used, transformed and/or transferred for the performance of the Services.

Security Incident: a breach of security that results in a real or imminent threat of unauthorised or unlawful access, use, disclosure, infringement, modification, theft, loss, corruption/alteration or destruction of EPSA MARKETPLACE Property/Customer Personal Data, interference with computer operations or interference with the functioning of the system. This covers, in particular, loss or theft of mobile devices, malfunctions, power failure, overloads, errors made by users/IT system staff, access violations, malware and hacking.

Security Policy: the security requirements for a system and/or an organisation;

- for an organisation, physical security requirements such as doors, locks, keys and walls;
- for systems, the constraints imposed on functions and the flows between them, and the constraints imposed on access by external systems, particularly programs, and on access to data by individuals.

Security Policy

The Supplier warrants that it has developed, implemented and will maintain and monitor a comprehensive written Security Policy containing security requirements for the sites, activities, personnel and systems used to develop, perform and deliver the Services /(e.g. ISO 27001, NIST).
The Supplier shall notify the Customer within one (1) month of any update to its Security Policy. In any event, the Supplier shall not reduce the level of security of the Services/Products.
The Customer may review the security policies and procedures on the Supplier's site, which may affect the performance of the Services/supply of the Products.
The Supplier shall comply with the latest version of EPSA MARKETPLACE's Information Protection as communicated by the Customer, applicable to the products, services and computer technologies delivered as part of the performance of the Services or necessary for the performance of the Services.

Organisation of information security

Prior to performance of the Services/Performance of the Order, the Supplier shall communicate to the Customer its governance rules concerning security and cybersecurity, including the points of contact and their responsibilities and tasks

Human Resources Security

The Supplier must ensure that its personnel are duly trained in the obligations incumbent upon them when processing the Customer's personal data.

Management of EPSA MARKETPLACE Property/Customer Personal Data

EPSA MARKETPLACE's Property remain the exclusive property of the Customer at all times. The Customer reserves the right to ask the Supplier to diligently amend, update, destroy or return, regardless of the manner, any Customer Property for which the Supplier is responsible.

The Supplier shall be able, at the Customer's request, to return and/or delete the Customer's Personal Data no later than one (1) month after the Customer's request.

The Supplier's service is equipped with an automatic deletion device for deleting the

Customer's personal data at the end of the data retention period.

The Supplier shall establish and maintain administrative, technical and physical safeguards to protect the security, integrity, confidentiality and availability of EPSA MARKETPLACE's Property and the Customer's Personal Data and, in particular, to protect EPSA MARKETPLACE's Property and the Customer's Personal Data against any threats or anticipated danger and to protect them against Security Incidents.

The Supplier shall maintain an inventory of all EPSA MARKETPLACE Property (or components supporting such Property).

The Supplier shall, upon request, provide reasonable assistance to the Customer to comply with all laws and regulations applicable to EPSA MARKETPLACE's Property and the Customer's Personal Data relating to, inter alia, identification, labelling, searching, de-identification, signposting, copying, modification, transfer and retrieval. In this case, the Supplier shall provide the Customer with any information they may require or that may prove necessary.

Access Control

The Supplier's administrators assume full responsibility for granting access to EPSA MARKETPLACE Property and Customer Personal Data to all of the Supplier's employees and other users, and for providing a process that will manage the secure and timely creation and deletion of employee and other user accounts. This process must include appropriate management approval, a verifiable history of all changes and an annual review of access authorisation and remediation of excessive access.
The Supplier shall establish, maintain and apply the security access principles of "Segregation of Duties", "Dual Control" and "Least Privilege" in relation to EPSA MARKETPLACE Property and the Customer's Personal Data.

The Supplier will record and keep logs of all accesses to EPSA MARKETPLACE's Property, the Customer's Personal Data and the Customer's information system by its staff, agents or subcontractors and these logs will be communicated to the Customer.

If the Supplier provides Services to the Customer from its premises, it will comply with the Prevention Plan communicated by the Customer insofar as it is applicable to the services and computer technologies delivered as part of the performance of the Services or necessary for the performance of the Services.

Physical and environmental security

In the case of Services carried out off Customer site connected EPSA MARKETPLACE's information system, the Supplier will indicate the geographical locations in which it operates EPSA MARKETPLACE's

Property and/or processes the Customer's Personal Data. In particular, the Supplier shall provide the address of their:

a. primary data centre and/or IT facility and,

b. backup and/or disaster recovery site.

Security of operations

The Supplier undertakes to use commercially supported software (e.g. software under active maintenance, including operating system, open source or application software and/or the like) on all systems that technically process, store or support the Services/the manufacture of the Products.
The Supplier shall notify the Customer one (1) year in advance of termination of commercial support for any component.
The Supplier shall notify the Customer one (1) year prior to the termination of commercial support for any component.

The Supplier will explain and detail its multi-client platform.

Systems acquisition, development and maintenance

The Supplier shall systematically use malware detection tools before any deliverable is delivered and shall provide the Customer with a report on the detection of such malware.

The rules for software development will include as a minimum:

a. no use of hard-coded identifiers;

b. separation of administrator and user roles;

c. systematic deletion of all default accounts used in the development process and modification of the default password before delivery to the Customer.

The Supplier shall provide documentary evidence on the following points concerning the design of the Products/performance of the Services:

a. the cyber-risks to which the Products and Services are exposed will be identified and will lead to the creation of appropriate cyber-security controls to be put in place;

b. reliable and unreliable data sources will be identified (for example, data sources internal to the Customer's organisation may be considered reliable, while other data sources may be considered unreliable).

The Supplier undertakes to carry out (at least annually) a vulnerability assessment of its systems accessing or containing EPSA MARKETPLACE Property and/or the Customer's personal data and will mitigate risks or remedy critical defects within an appropriate timeframe having regard to the importance of the defect and the workload required for remediation. The Supplier undertakes to provide the Customer with reports specifying the date of the assessment, the identity of the persons who carried out the assessment and an indication of the risk relating to the vulnerabilities identified as well as the time required to remedy them. The vulnerability threat assessment will be carried out using industry-standard tools and/or services.

The Supplier will implement a process for controlling technical modifications to software and hardware products.

Security Incident Management

The Supplier will implement a thorough and agreed Security Incident Management process for the networks and systems it operates, including the identification, response, containment, recovery, reporting, evidence protection and review of Security Incidents.

The Supplier undertakes to inform the Customer without delay of the occurrence of an event, no later than twenty-four (24) hours after becoming aware of a Security Incident, at the following address: Contact@epsa-marketplace.com. The notification must include at least:

a. a statement or description of the problem;
b. the expected remediation period (if known);
c. the name and telephone number of the Supplier's representative whom the Customer may contact to obtain further information.

Evidence relating to a Security Incident will be collected, kept and presented by the Supplier in order to comply with the rules of evidence applicable before the competent courts.

Business continuity management

The Supplier shall have deployed the means to ensure business continuity and disaster recovery, including the resilience of the Services/Products delivered to the Customer.

The Supplier shall notify the Customer in the event of a claim.

Compliance

The Supplier acknowledges that the Customer or an independent auditor appointed by the Customer may, at its own expense, carry out an audit of the Supplier's compliance with its security commitments on its systems, processes and procedures and supply chain, affecting the Customer's Services/Products or systems. This includes, in particular, verifying agreement and access control, controlling the flow of information and audit logs. The Supplier will provide all the necessary documentation and proof.
Due to the confidential and exclusive nature of the Supplier's operations, and in order to protect the integrity and security of such operations and the shared nature of the systems that may be used to provide the Services/Products:

- the parties will agree in advance on the scope of the audits;
- at least thirty (30) days' written notice shall be given by the Customer prior to the date on which the audit is due to commence and the audit shall take place no more than once in any twelve (12) month period, unless there are circumstances such as a reasonable suspicion on the part of the Customer of a Security Incident, in which case an audit may be carried out on a date mutually agreed by the parties;
- if the audit is carried out by a third party, the latter shall be an expert auditor in the field of security and approved by the parties, it being understood that the Supplier may not refuse the third party auditor without a legitimate reason;

- the audit will be conducted in accordance with the confidentiality and non-disclosure requirements and constraints of the parties; and
- the audit must not unreasonably disrupt the Supplier's normal business or IT operations.

Notwithstanding the provisions above, the Customer retains the discretion to initiate a security inspection under this section, and may initiate the inspection prior to the performance of the Services/delivery of Products and thereafter, (i) in the event of any change in the performance of the Services/delivery of the Products which may affect the security thereof, (ii) following any Security Incident affecting the Services or EPSA MARKETPLACE's Property or the Customer's Personal Data, and (iii) in the event of a request from the Customer or a request from a government agency. The Supplier shall provide the Customer with such reasonable assistance as may be necessary to enable the Customer to comply with applicable security laws.

The Supplier shall keep and protect any proof of compliance with legal or contractual obligations and shall make such proof available to the Customer if necessary