Security Requirements

The Vendor understands and acknowledges the importance of ensuring the security of Deltatre information irrespective of whether such information is in digital, paper or other form. This annex describes Deltatre minimum information security requirements (updated from time to time), which the Vendor is required to comply with in relation to its processing of Deltatre information. The Vendor will be responsible for any breach of these requirements by itself and its employees, its subcontractors and other subjects the Vendor does business with and will indemnify and keep Deltatre harmless for any liability and costs occurred in connection with any of the such breaches. The Vendor acknowledges that failure to comply with these minimum information security requirements will amount to a material breach of the contract entered between Deltatre and the Vendor and will entitle Deltatre to immediately terminate such contract.

For the purpose of this Annex, "i**nformation** is any information owned, processed or held by Deltatre, irrespective of storage location. Information is used interchangeably with the term "data". It includes information on business operations, proposed changes, plans, and other corporate information and reports.

1- INFORMATION SECURITY POLICY

The Vendor must have in place an Information Security Policy framework which complies with applicable laws and regulations, is constantly up-to-date and meets applicable industry standards. The Vendor must review its policy periodically (at least yearly) and must ensure that all employees, as well as relevant subcontractors:

- Have been validated for trustworthiness (by screening or other accepted procedures) and have signed NDAs.
- Receive periodic security awareness training and understand their responsibility to exercise due care.
- Read the Vendor policy, agree to adhere to it in writing and comply with all technical and organizational security measures established to protect confidential information.

In the event that the Vendor does not have in place its own information security policy, the Vendor will be required to comply with the Deltatre Group Information Security Policy, which will be provided as needed.

2- INFORMATION SECURITY BEST PRACTICES

The Vendor must be able to demonstrate that it follows security best practices in the processing of Deltatre confidential data.

Examples of this include (but are not limited) to:

- securely configured infrastructure devices, technical systems cloud platforms (and integrations to and from) and applications as per manufacturer's specifications;
- have in place a reliable and up to date antivirus system;
- use currently licensed and fully maintained software;
- regularly and promptly apply security updates to electronic devices, systems, and software;

- complete periodic penetration testing and vulnerability management for systems and infrastructure;
- use secure software development practices, such as defence-in-depth design, enforcement of separation of duties, employment of least privilege, embed non-repudiation, design for secure error/failure and separation of production software & data from development, requiring approval before any changes to software or data are made, properly testing the security of all approved changes, amongst others;
- have in place and diligently use secure encryption and manage firewalls, intrusion detection systems, logging and monitoring and other such industry standard IT security technologies;
- have in place mechanisms to continue critical services in the event of a disaster (e.g. Disaster Recovery Plans & Tests);
- isolate all Deltatre confidential information from all other supplier's or customer's information either (i) by separating physical servers or when this is not possible (ii) by using logical separation (e.g. separate protected database or table) combined with logical access controls (i.e. encryption keys, etc.).

3- COMMUNICATION OF INFORMATION

The Vendor must ensure all personal and confidential information is:

- sent and received through secure communication channels and only by authorized personnel, with a need to know. If personal and/or confidential information is transmitted, strong encryption is required. All data at rest and in transit shall be encrypted. For data in transit only secure encryption methods (not deprecated) must be used. Symmetric key lengths to be at least 256 bits and asymmetric key lengths to be at least 2048 bits, secure renegotiation to be used and compression disabled
- deleted from the communication mechanism (e.g. Secure FTP, email, file share, collaboration websites, etc.) when no longer necessary (accumulation of files over time should be avoided if not necessary);
- delivered by hand, by registered mail with request for receipt or courier services, if communication is on paper or other physical media;
- properly secured and periodically tested, if communication requires remote access or permanent interfaces (with supplier or Client systems), such access or interface must be approved by Deltatre Security Department.

4- ACCESS RIGHT MANAGEMENT

The Vendor must ensure that all access rights' accounts or credentials (including physical access badges) should:

- only provide access to trustworthy personnel subject to confidentiality agreements;
- be for a named person and not for a generic shared account;
- be kept up to date ensuring that any Vendor or Deltatre personnel changes (leavers, movers) are made immediately;
- use strong passwords and update them regularly (at least every 3 months). Password shall : be a minimum eight characters (from 16-char to 64-char for users/roles with administrative access); Contain at least one

letter, one number, one special character; Contain at least one uppercase letter and one lowercase letter; not contain user first name, last name, username, or combinations of; have no more than two identical characters in a row. In case of absence of Multi-Factor Authentication methodology the 'never expire' flag must be turned off, where present. Password history used by users shall be kept to disallow re-entering a previously used password. Where possible credentials should be checked against password stuffing and data-breaches archives;

- implement Single Sign On or Multi-Factor Authentication, unless specifically authorized otherwise in writing by Deltatre;
- cover only the access required to perform the authorized activities and not more;
- have in place “timeouts” (not less than 15 minutes) for accessing electronic devices and confidential information.

5- INCIDENTS

The Vendor will immediately notify Deltatre of any incidents affecting the confidentiality, integrity or availability of Deltatre information in accordance with the criticality and escalation table below.

In addition to notifying your business contact at Deltatre, please notify Deltatre Security team following the escalation path described in the Appendix A – Incident Critically Levels & Escalation Path presents in this document.

6- STORAGE OF PERSONAL AND CONFIDENTIAL INFORMATION

The Vendor shall ensure that all storage locations and media is:

- maintained and managed in a secure physical location accessible only by authorized persons;
- if on a network or cloud platform, be in a secure location (preferably not accessible from the Internet) and only accessible by authorized persons. The Vendor must comply with the data retention as required by Deltatre (since each Company of the Group has its own data retention policy, the supplier shall comply with the specific indications provided by the company with which the supply contract is in place) and it must not permit storage of Deltatre personal and confidential information on free e-mail accounts (i.e. Yahoo, Gmail, etc.) and free cloud file sharing services;
- if on removable media (i.e. USB key or other) the information should be encrypted with a strong algorithm, such as AES256. Encryption keys must be separately, and securely stored and exchanged;
- if required for the particular service, the Vendor shall ensure encrypted backups are maintained in a secure location (preferably offsite).

7- PERSONAL AND CONFIDENTIAL INFORMATION DISPOSAL AND END OF ENGAGEMENT

For any personal and confidential information no longer needed and at the end of every contract or specific project, the Vendor must:

- securely return to Deltatre any information provided by Deltatre following the end of the engagement or service within an agreed timeframe;
- delete digital information so that it is no longer accessible, including any backups (i.e. removable media, email, file servers, etc.) and securely destroy all media on assets being decommissioned; or -if not possible- render all information on such media irrecoverable prior to the decommissioning or disposal of the asset, this must be carried out within an agreed timeframe;
- share (cross-cut shredder preferably), securely destroy or return any paper documents to Deltatre, including any documents stored in physical archives within an agreed timeframe;
- certify in writing to Deltatre that the foregoing has been done.

8- CREDIT CARD PROCESSING

If the product or service provided by the Vendor will directly or indirectly handle any form of credit card information (i.e. credit card number, cardholder name, expiration date, surname, card verification values, etc.), the Vendor shall demonstrate its full compliance with the Payment Card Industry Data Security Standard (PCI DSS) valid at the time. According to its PCI DSS classification level, the Vendor shall provide its valid certificate or the relevant self-assessment questionnaire on a yearly basis.

9- COMPLIANCE ASSESSMENT

Deltatre may verify compliance with the above as part of the initial setup of the supplier products or services, annually or following an incident. As part of the compliance verification process, Deltatre may ask to the Vendor to present any security certifications (e.g.: ISO-27001 Certificate or SSAe16 reports) or ask to provide a security assessment that will be performed by Deltatre Security Team on the Vendor infrastructure/service.

APPENDIX A

INCIDENT CRITICALITY LEVELS & ESCALATION PATH

INCIDENT CRITICALITY	ESCALATION
Critical Risk Level: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed, such as – without being limited to- an attack or error effectively allowed an unauthorized third party, for example, to gain full control over the system containing Client Information or directly of the Client information itself.	**Priority 0:** Joint Vendor/ Deltatre Security Incident Response Team. Deltatre Contacts: • IT Team: Technology.CorporateIT@deltatre.com • Security Team: security@deltatre.com • Data Breach Team: Data.breach@deltatre.com
High Risk Level: An attack or error which could have allowed an unauthorized third party: • Access to Deltatre client information (one or more - including Client). • Circumvent access restrictions to get access to personal or confidential information. • Access Client personal or confidential data due to the lack of sufficient security in the communication channels used.	**Priority 1:** Joint Vendor/Deltatre Security Incident Response Team. Deltatre Contacts: • IT Team: Technology.CorporateIT@deltatre.com • Security Team: security@deltatre.com • Privacy Team: privacy@deltatre.com
Medium Risk Level: An attack or error which affects core functions of the service or product provided, but which does not compromise the system in general.	**Priority 2:** Joint Vendor/ Deltatre IT Team • IT Team: Technology.CorporateIT@deltatre.com
All other incidents of lower importance.	**Priority 3:** Handling by supplier internal incident management team.