

## Supplier IT Security Policy

Tecknuovo Limited (Tecknuovo)

INTERNAL

### 1. Introduction

- 1.1 This document sets out the measures to be taken by all suppliers and their staff (**Suppliers**) when delivering services to Tecknuovo in order to protect the computer systems, devices, infrastructure, computing environment and any and all other relevant equipment of the Suppliers, Tecknuovo and any customer of Tecknuovo (**Customer**) (collectively, **IT Systems**) from damage and threats whether internal, external, deliberate, or accidental.
- 1.2 This policy sets out the minimum requirements of the Supplier the Supplier shall comply with in addition to any other information systems and/or security standards of Tecknuovo set out in the Supplier Use of Device Policy, Supplier Code of Conduct, Data Processor terms and conditions, and all other policies issued to the Supplier from time to time (**Information Policies**).
- 1.3 The Supplier must also adhere to any specific standards required by Tecknuovo for any Customer for a project with respect to the IT Systems.
- 1.4 All Suppliers and their staff and any and all third parties authorised to use the IT Systems including, but not limited to, contractors and sub-contractors of the Supplier (collectively, **Users**), must ensure that they are familiar with this Policy and must adhere to and comply with it at all times.

### 2. Key Principles

- 2.1 The Supplier shall ensure that it and any Users comply with the following principles in respect of its own IT Systems, and those of Tecknuovo and/or any Customer that it and or its Users have access to in the provision of its services to Tecknuovo.
- 2.2 All data stored on IT Systems must be managed securely in compliance with the Data Protection Act 2018 UK GDPR, and such parts of EU Regulation 2016/679 General Data Protection Regulation and all other laws governing data protection whether now or in the future in force that apply to processing of data in the United Kingdom (UK) (**Data Protection Legislation**).
- 2.3 All data stored on IT Systems must be classified appropriately (including, but not limited to, personal data, sensitive personal data, and confidential information). All data must be handled appropriately in accordance with its classification.
- 2.4 All data stored on IT Systems shall be available only to those Users with a legitimate reason and need for access.
- 2.5 All data stored on Supplier IT Systems shall be protected against unauthorised access and/or processing.
- 2.6 All data stored on Supplier IT Systems shall be protected against loss and/or corruption.
- 2.7 All Supplier IT Systems must be maintained, serviced, repaired, and upgraded by the Supplier.
- 2.8 The Supplier remains responsible at all times for the security and integrity of all Supplier IT Systems and the data stored thereon (including, but not limited to, the security, integrity, and confidentiality of that data).
- 2.9 The Supplier shall report any and all breaches of security pertaining to the Supplier's IT Systems or any data stored thereon to Tecknuovo and the Supplier shall ensure where this relates to its own IT System that it subsequently investigates the breach and keeps Tecknuovo informed as to the outcome of such

investigation, any risk to data belonging to Tecknuovo and or any Customer, and the steps taken by the Supplier to rectify the breach and prevent the same breach re-occurring.

- 2.10 If the Supplier suspects a breach has occurred involving the IT Systems of Tecknuovo and/or the Customer, and whether or not the Supplier or any User is the cause of or has been involved in such breach, the Supplier shall notify Tecknuovo immediately it becomes aware of or suspects a breach.

### 3. Supplier Responsibilities

3.1 The Supplier shall be responsible for the following:

- a) ensuring that all Supplier IT Systems are assessed and deemed suitable for compliance with Tecknuovo's security requirements where such IT Systems will be utilised and or where personal data or any other data belonging to Tecknuovo, the Customer or any third party in the provision of the services by the Supplier to Tecknuovo and or the Customer;
- b) ensuring that IT security standards are effectively implemented for the Supplier IT Systems and regularly reviewed, working in consultation with Tecknuovo's senior management and Data Protection Officer, as appropriate, and reporting the outcome of such reviews to Tecknuovo's senior management;
- c) ensuring that the Supplier IT Systems meet the security standards and requirements of Tecknuovo set out in the Supplier Use of Device Policy, Supplier Code of Conduct and data processing agreement the Supplier has entered into;
- d) ensuring that all Users are kept aware of the requirements of this Policy, any other Tecknuovo policies in respect of the same subject matter and of all related legislation, regulations, and other relevant rules whether now or in the future in force including, but not limited to, data protection laws and the Computer Misuse Act 1990.

3.2 The Supplier shall ensure that its access to and/or use of any IT Systems of Tecknuovo or the Customer is undertaken in accordance with the principles and obligations of this Policy together with the terms and conditions of the Information Policies.

3.3 The Supplier shall be responsible for the following:

- a) ensuring all Users understand and comply with this Policy and all other Information Policies and any specific standards required by any Customer as notified to the Supplier;
- b) providing all Users with appropriate support and training in IT security matters, data protection, and use of IT Systems;
- c) ensuring that all Users are granted levels of access to IT Systems that are appropriate for each User, taking into account their job role, responsibilities, and any special security requirements;
- d) receiving and handling all reports relating to IT security matters and taking appropriate action in response;
- e) taking proactive action, where possible, to establish and implement IT security procedures and raise User awareness;
- f) assisting Tecknuovo in monitoring all IT security in respect of the delivery of the services of the Supplier and taking all necessary action to implement this Policy and any changes made to this Policy in the future; and
- g) ensuring that regular backups are taken of all data stored within the Supplier IT Systems at intervals no less than daily and that such backups are stored at a suitable location. All backups should be encrypted.

## 4. Users' Responsibilities

- 4.1 The Supplier shall ensure the Users are contractually required to comply with the following obligations and shall use all reasonable endeavours to enforce the same.
- 4.2 All Users must comply with all relevant parts of this Policy and any Information Policies at all times when using the IT Systems.
- 4.3 All Users must use the IT Systems only within the bounds of UK law and must not use the IT Systems for any purpose or activity which is likely to contravene any UK law whether now or in the future in force.
- 4.4 Users must immediately inform the Supplier's IT Department (and, where such concerns relate to personal data, the Data Protection Officer) of any and all security concerns relating to the IT Systems. Where such concerns relate to Tecknuovo's or the Customer's IT Systems, the Supplier shall in turn report the same to Tecknuovo's management and Data Protection Officer.
- 4.5 Users must immediately inform the relevant IT Department of any other technical problems (including, but not limited to, hardware failures and software errors) which may occur on the IT Systems.

## 5. Software Security Measures

- 5.1 All software in use on the Supplier's IT Systems (including, but not limited to, operating systems, individual software applications, and firmware) will be kept up-to-date and any and all relevant software updates, patches, fixes, and other intermediate releases will be applied by the Supplier. This provision does not extend to upgrading software to new 'major releases' (e.g. from version 1.0 to version 2.0), only to updates within a particular major release (e.g. from version 1.0 to version 1.0.1 etc.). Unless a software update is available free of charge it will be classed as a major release, falling within the remit of new software procurement and outside the scope of this provision.
- 5.2 Where any security flaw is identified in any software that flaw will be either fixed immediately or the software may be withdrawn from the Supplier's IT Systems until such time as the security flaw can be effectively remedied. If the security flaw affects, is likely to affect, or is suspected to affect any personal data, the Data Protection Officer shall be informed immediately.
- 5.3 The Supplier shall ensure no Users may install any software of their own, whether that software is supplied on physical media or whether it is downloaded, to its IT Systems without the approval of the Supplier's IT department. All software will be installed onto the IT Systems by the IT Department.

## 6. Anti-Virus Security Measures

- 6.1 All Supplier IT Systems (including all computers and servers) will be protected with suitable anti-virus, firewall, and other suitable internet security software. All such software will be kept up-to-date with the latest software updates and definitions.
- 6.2 All IT Systems protected by anti-virus software will be subject to a full system scan at regular intervals and in accordance with any recommendations of the Information Commissioner under any published codes on security matters relating to data protection.
- 6.3 All physical media (e.g. USB memory sticks or disks of any kind) used by Users for transferring files must be virus-scanned before any files may be transferred. The Supplier shall not allow any Users to use such physical media to access Tecknuovo's and or the Customer's IT Systems to transfer files, unless express written permission has been given by the relevant party.
- 6.4 Users shall be permitted to transfer files using cloud storage systems only with the approval of the Supplier's own IT department, and where files relate to Tecknuovo and or the Customer, only with the express written permission of Tecknuovo. All files downloaded from any cloud storage system must be scanned for viruses during the download process. The Supplier acknowledges that it is required to adhere to the additional requirements of the Supplier Use of Device Policy with respect to the storing of data on its IT Systems.
- 6.5 Any files sent to third parties outside the Supplier's IT System, whether by email, on physical media, or by

other means (e.g. shared cloud storage) must be scanned for viruses before being sent or as part of the sending process, as appropriate. All email attachments are scanned automatically upon sending.

- 6.6 Where any virus is detected by a User this must be reported immediately to the Supplier IT Department (this rule shall apply even where the anti-virus software automatically fixes the problem). The IT Department shall promptly take any and all necessary action to remedy the problem. In limited circumstances this may involve the temporary removal of the affected computer or device. Where such virus may or could affect the IT Systems of Tecknuovo and/or the Customer, the Supplier shall notify Tecknuovo immediately.
- 6.7 If any virus or other malware affects, is likely to affect, or is suspected to affect any personal data of Tecknuovo and/or the Customer, in addition to the above, the issue must be reported immediately to Tecknuovo.
- 6.8 Where any User deliberately introduces any malicious software or virus to the IT Systems this will constitute a criminal offence under the Computer Misuse Act 1990 and will be handled as appropriate under the Supplier's disciplinary procedures. The Supplier shall ensure that all such instances which affect or may affect Tecknuovo and or the Customer or their IT Systems are reported immediately to Tecknuovo.

## 7. Hardware Security Measures

- 7.1 Wherever practical, Supplier IT Systems will be located in rooms which may be securely locked when not in use or, in appropriate cases, at all times whether in use or not (with authorised Users being granted access by means of a key, smart card, door code or similar). Where access to such locations is restricted, Users must not allow any unauthorised access to such locations for any reason.
- 7.2 All Supplier IT Systems not intended for normal use by Users (including, but not limited to, servers, networking equipment, and network infrastructure) shall be located, wherever possible and practical, in secured, climate-controlled rooms and/or in locked cabinets which may be accessed only by designated members of the IT Department.
- 7.3 No Users shall have access to any IT Systems not intended for normal use by Users (including such devices mentioned above) without the express permission of the IT Department, whether of the Supplier, Tecknuovo and or the Customer. Under normal circumstances, whenever a problem with such IT Systems is identified by a User, that problem must be reported to the IT Department. Under no circumstances should a User attempt to rectify any such problems without the express permission (and, in most cases, instruction and/or supervision) of the IT Department.
- 7.4 All non-mobile devices (including, but not limited to, desktop computers, workstations, and monitors) utilised by the Supplier and its Users shall, wherever possible and practical, be physically secured in place with a suitable locking mechanism. Where the design of the hardware allows, computer cases shall be locked to prevent tampering with or theft of internal components.
- 7.5 All mobile devices (including, but not limited to, laptops, tablets, and smartphones) provided by Tecknuovo or the Customer should always be transported securely and handled with care. In circumstances where such mobile devices are to be left unattended they should be placed inside a lockable case or other suitable container. Users should make all reasonable efforts to avoid such mobile devices from being left unattended at any location other than their private homes or Company premises. If any such mobile device is to be left in a vehicle it must be stored out of sight and, where possible, in a locked compartment.

## 8. Access Security

- 8.1 Access privileges for all IT Systems shall be determined on the basis of Users' levels of authority within the Supplier, Tecknuovo, the Customer and the requirements of their roles. Users shall not be granted access to any IT Systems or electronic data which are not reasonably required for the fulfilment of their roles.
- 8.2 All IT Systems (and in particular mobile devices including, but not limited to, laptops, tablets, and smartphones) shall be protected with a secure password or passcode, or such other form of secure log-in system as the IT Department may deem appropriate and approve. Not all forms of biometric log-in are

considered secure. Only those methods approved by the IT Department may be used.

- 8.3 All passwords must, where the software, computer, or device allows:
- a) be at least 10 characters long;
  - b) contain a combination of <<upper and lower case letters / numbers / spaces / symbols etc.>>;
  - c) be different from the previous password;
  - d) not be obvious or easily guessed (e.g. birthdays or other memorable dates, memorable names, events, or places etc.); and
  - e) be created by individual Users.
- 8.4 Passwords should be kept secret by each User. Under no circumstances should a User share their password with anyone. No User will be legitimately asked for their password by anyone at any time and any such request should be refused. If a User has reason to believe that another individual has obtained their password, they should change their password immediately and report the suspected breach of security to the IT Department and, where personal data could be accessed by an unauthorised individual, the Data Protection Officer.
- 8.5 If a User forgets their password, this should be reported to the IT Department. The IT Department will take the necessary steps to restore the User's access to the IT Systems which may include the issuing of a temporary password which may be fully or partially known to the member of the IT Staff responsible for resolving the issue. A new password must be set up by the User immediately upon the restoration of access to the IT Systems.
- 8.6 Users should not write down passwords if it is possible to remember them. If a User cannot remember a password, it should be stored securely (e.g. in a locked drawer or in a secure password database) and under no circumstances should passwords be left on display for others to see (e.g. by attaching a note to a computer display).
- 8.7 All IT Systems with displays and user input devices (e.g. mouse, keyboard, touchscreen etc.) shall be protected, where possible, with a password protected screensaver that will activate after 5 minutes of inactivity. This time period cannot be changed by Users and Users may not disable the screensaver. Activation of the screensaver will not interrupt or disrupt any other activities taking place on the computer (e.g. data processing).
- 8.8 Users may not use any software which may allow outside parties to access the IT Systems without the express consent of the IT Department. Any such software must be reasonably required by the User for the performance of their job role and must be fully inspected and cleared by the IT Department and, where such access renders personal data accessible by the outside party, the Data Protection Officer.
- 8.9 Where the Supplier is required to use Supplier devices, Users may connect such devices (including, but not limited to, laptops, tablets, and smartphones) to Tecknuovo or Customer networks subject to the approval of the IT Department. Any and all instructions and requirements provided by the IT Department governing the use of Users' own devices when connected to Tecknuovo or Customer network must be followed at all times. Users' use of their own devices shall be subject to, and governed by, all relevant Information Policies while those devices are connected to Tecknuovo network or to any other part of the IT Systems. The IT Department shall reserve the right to request the immediate disconnection of any such devices without notice.

## 9. Data Storage Security

- 9.1 All data, and in particular personal data, should be stored securely using passwords and data encryption.
- 9.2 All data stored electronically on physical media, and in particular personal data, should be stored securely in a locked box, drawer, cabinet, or similar.

- 9.3 No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to Tecknuovo, the Customer or otherwise.

## 10. Access, Use of and Storage of Government data (if applicable)

- 10.1 The Supplier may deliver services to Customers who are Government departments and as such the Supplier must ensure it is familiar with and complies with all policies and rules regarding access, use and or storage of Government data as may apply to such Government department. All Government data carries one of the following 3 security classifications:

- OFFICIAL
  - OFFICIAL - SENSITIVE
- SECRET
- TOP SECRET

- 10.2 Within the classification of OFFICIAL, there is an additional category of OFFICIAL-SENSITIVE for information which is considered sensitive OFFICIAL information. OFFICIAL-SENSITIVE requires more stringent handling procedures and handling on a strict 'need to know'. As a consequence, there are more rigorous rules applying to the use of non-Government devices (includes but is not limited to laptops, tablets, mobile phones) of suppliers with Government data, access to Government data, and the storage of such Government data on non-Government device where such data is classified at OFFICIAL-SENSITIVE and above.

- 10.3 The Supplier will ensure that it and its Users familiarise themselves with and comply with the principles of the Government Security Classifications publication v1.1 May 2018, Working with OFFICIAL information publication, FAQ Sheet 2: Managing Information Risk at OFFICIAL, and such other related advice and publications as to managing risk and use of Government data as are published from time to time and stored within the Government Security Classification section of publications which can be found at: <https://www.gov.uk/government/publications/government-security-classifications>.

- 10.4 Subject to clause 10.6 below, the Supplier may use non-Government devices to undertake services at the OFFICIAL classification only, as long as the devices meet the security requirements of the respective Government department and are used in accordance with the Government department's acceptable use policy. For all Government information which is classified as OFFICIAL - SENSITIVE or within SECRET and or TOP SECRET, the Supplier shall not use their own devices to access, use and or store such Government data, unless such devices are contractually approved by Tecknuovo in conjunction with the Government department concerned.

- 10.5 Subject to clause 10.6, where the Supplier may use its own devices in respect of any work for a Government department, it must not and ensure all Users do not connect their devices to the Government department's computer network, unless otherwise approved by the Government department concerned and notified by Tecknuovo. The Supplier may be entitled to store OFFICIAL Government data using certain approved online storage and or digital tools, where notified by Tecknuovo and or the Customer and in accordance with any Customer policy.

- 10.5 The Supplier and its Users will comply with all specific rules and policies of any Government department who is a Customer of Tecknuovo regarding access to, the use of and storage of data for that Government department, which shall be notified to the Supplier by Tecknuovo as part of any Customer policy pack issued in respect of the delivery of services to such Customer.

## 11. Data Protection

- 11.1 All personal data of Tecknuovo or the Customer collected, held, and processed by the Supplier will be collected, held, and processed strictly in accordance with the principles of data protection laws applicable to the UK and the Information Policies.

- 11.2 All Users handling data for and on behalf of Tecknuovo shall be subject to, and must comply with, the provisions of the Data Sub-Processor Agreement at all times. In particular, the following shall apply:
- a) All emails containing Customer Data (as defined in the Data Sub-Processor Agreement) must be encrypted and marked "confidential";
  - b) Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted under any circumstances;
  - c) Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
  - d) Personal data contained in the body of an email, whether sent or received, should be copied directly from the body of that email, and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted;
  - e) All personal data to be transferred physically, including that on removable electronic media, shall be transferred in a suitable container marked "confidential".
  - f) Where any confidential or personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the User must lock the computer and screen before leaving it.
- 11.3 Any questions relating to data protection should be referred to the Data Protection Officer.

## 12. Internet and Email Use

- 12.1 All Users shall be subject to and must comply with and any other Tecknuovo policies regarding the use of communications, email and internet in the provision of the Supplier's services.
- 12.2 Where provisions in this Policy require any additional steps to be taken to ensure IT security when using the internet or email over and above the requirements imposed by any other Information Policies, the Supplier must take such steps as required.

## 13. Reporting IT Security Breaches

- 13.1 All concerns, questions, suspected breaches, or known breaches that involve personal data of Tecknuovo and/or the Customer shall be referred immediately to Tecknuovo who shall handle the matter in accordance with Tecknuovo's Data Protection Policy.
- 13.2 Under no circumstances should a User attempt to resolve an IT security breach on their own where the same relates to personal data of Tecknuovo and or the Customer without first consulting Tecknuovo.
- 13.3 All IT security breaches shall be fully documented.

## 14. Policy Review

Tecknuovo shall review this Policy on an annual basis and otherwise as required in order to ensure that it remains up-to-date and fit for purpose. All questions, concerns, and other feedback relating to this Policy should be communicated to the Supplier's project manager at Tecknuovo.

## 15. Implementation of Policy

This Policy shall be deemed effective as of 1 January 2021. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

## 16. Failure to comply with this policy

Failure to comply with this policy may result in the termination of any statement of work, including, where appropriate, revocation of access to the IT systems, and criminal prosecution in accordance with local laws. As well as any specific rights Tecknuovo has in this policy that apply where the Supplier breaches particular provisions of this policy, the Supplier's breach of its obligations under this policy will constitute a breach of its contract with Tecknuovo and

Tecknuovo may exercise its rights under that contract. If you have reasonable grounds to suspect that someone else is in breach of this policy, you must inform Tecknuovo immediately.