POLICY OBJECTIVES

- To protect the information that Tecto Ltd handles, stores, exchanges, processes and has access to, and to ensure the ongoing maintenance of its confidentiality, integrity and availability.
- To ensure controls are implemented that provide protection for information and that they are proportionate to their value and the threats to which they are exposed.
- To ensure that Tecto Ltd complies with all relevant legal, customer and other third party requirements relating to information security and the protection of personal information.

POLICY

EMAILS

- Employees must apply extreme caution when opening emails and/or attachments received from unknown senders. If in doubt, they should move the email to their junk folder and report it to ICT Director.
- Employees must not send unsolicited, unauthorised or illegal materials to any individual.
- Employees must not use company email accounts to send emails that are not related to their work.

PASSWORDS

- Access to all company-owned electronic devices (including removable media) must require the submission of either a password or fingerprint ID.
- All passwords must be unique to each individual employee and they must not under any circumstances be shared or disclosed by an employee to any other person.

All passwords:
Are not to contain the user's account name or parts of the user's full name that exceed two consecutive characters

- Be at least eight characters in length
- Contain characters from three of the following four categories:
- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Base 10 digits (0 through 9)
- Non- alphabetic characters (for example !, $, #, %)

USE OF COMPANY EQUIPMENT (desktops, laptops, tablets, phones, removable media, servers)

- A record of every item of company equipment issued to an employee must be maintained by the ICT Director.
- The use of all company equipment will be monitored by ICT Director.
- All company equipment used to store information must be encrypted and protected with up-to-date anti-malware software.
- Removable media must only be used to store and transfer data and only with the written authorisation of ICT Director.
- All equipment must be completely cleared of any stored information prior to its disposal.
- Employees must not:
    - Use any company equipment that has not been issued to them without written authorisation from ICT Director;
    - Allow any other individual to use any company equipment that has been issued to them without written authorisation from ICT Director;
    - Deliberately cause damage to any company equipment, including maliciously deleting, corrupting or restricting access;
    - Allow company equipment to be used to maliciously delete, corrupt or restrict access to any the information accessed using it;
    - Deliberately introduce viruses or other harmful sources of malware onto company equipment;
    - Use company equipment to access external websites or networks that they have not been authorised to access and are not related to the company's activities;

TectoGroup
Unit 2 Spinney View,
Round Spinney Ind Est
Northampton NN3 8RF

T 01604 961 961
E info@tecto.co.uk
W www.tecto.co.uk

Registered in England & Wales No: 07923637

- Use company equipment to knowingly access, download or store materials from the internet that are illegal, immoral, unethical or deemed to be indecent or gross in nature;
- Use company equipment to send unsolicited, unauthorised or illegal materials to any internal or external recipient;
- Install software onto any company equipment without written authorisation from ICT Director;
- Modify, delete or remove software from any company equipment without written authorisation from ICT Director;
- Attempt to bypass or over-ride any controls used to monitor the use of company equipment;
- Attempt to bypass or over-ride any back-up processes;
- Use any company equipment for any personal reasons, other than those authorised by the ICT Director;
- Leave any company equipment unattended in an unsecure area;
- Use or store any company equipment in environments or areas where there is a reasonable risk of them becoming damaged by impact, water ingress, extreme temperatures or electromagnetic fields.

EMPLOYEES MUST

- Ensure that access to any company equipment they use is ocked down with a screen saver or equivalent whenever they leave it unattended;
- Report to ICT Director whenever they suspect company equipment has been infected with a virus or malware or accessed by another person;
- Report to ICT Director whenever they suspect the antimalware and/or encryption software applied to any company equipment is not working correctly or has been compromised;
- Report to ICT Director whenever they suspect a back-up process has not been completed successfully;
- Immediately report to ICT Director if any company equipment is known or suspected to be lost or stolen;
- Ensure company equipment is carried as hand luggage when travelling.

LINE MANAGERS MUST

- Ensure that any equipment issued to employees who report to them is returned immediately:
- If they are suspended from their duties;
- Before they leave the company;
- Before commencing any "Gardening Leave" or any temporary leave of absence (e.g. maternity leave);
- Recorded using a Termination Checklist.
- Notify ICT Director as soon as they receive formal notice from an employee to terminate their employment. QA Coordinator will then decide whether any equipment issued to the employee should be returned whilst they complete their notice period.

ACCESS TO INFORMATION

- ICT Director will, as far as is reasonably practical, ensure that access to any information stored or processed by the company is automatically logged in every instance and that these logs are protected and retained for a minimum of 3 months.
- Any access privileges provided to an employee to any software system or application, network driver, electronic or hard copy folders/files must be authorised in writing by ICT Director
- Employees must not:
  - Attempt to access any software system or application, network driver, electronic or hard copy folders/files that they have not received formal authorisation to access from ICT Director. In particular, they should not attempt to access the following without authorisation:
  - Information relating to customers, suppliers or other third parties who they do not have any dealings with or is not required for them to fulfil their role or responsibilities;

TectoGroup
Unit 2 Spinney View,
Round Spinney Ind Est
Northampton NN3 8RF
T 01604 961 961
E info@tecto.co.uk
W www.tecto.co.uk
Registered in England & Wales No: 07923637

- Commercially sensitive information relating to contracts, proposals, orders, payments, confidential meetings or invoices;
- Information relating to employees that is not required for them to fulfil their role or responsibilities;
- Attempt to bypass or over-ride any controls used to monitor access to information;
- Store information anywhere other than the designated software or folder for that type/category of information;
- Share or distribute any information (including by email) to individuals if they are not aware whether the individual has been granted access to it.

Employees must:

- Immediately report any instances to ICT Director where they identify or suspect that they have been given access to information that is not relevant to their role or responsibilities;
- Immediately report any instances to ICT Director where they identify or suspect that they have the ability to modify or delete any information that is not relevant to their role or responsibilities;
- Avoid, as far as possible, emailing information in the form of spreadsheets or editable documents.
- Wherever possible, information should be shared in the form of links to the location where the information is stored.
- Line managers must ensure that access to information by any employees who report to them is revoked immediately:
- If they are suspended from their duties;
- Before they leave the company;
- Before commencing any "Gardening Leave" or any temporary leave of absence (e.g. maternity leave).

Line managers must:

- Notify ICT Director as soon as they receive formal notice from an employee to terminate their employment. QA Co-ordinator will then decide whether any changes need to made to the employee's access privileges while they complete their notice period.
- Notify ICT Director if any employee changes role. QA Co-ordinator will then decide whether any changes need to be made to the employee's access privileges.

ACCESS TO TECTO'S SITE/BUILDINGS

- Access to the Company's server room is restricted to individuals authorised by ICT Director.
- Employees must not:
  - Attempt to access any rooms or site areas that have controlled access unless they have been granted access to them by their Line Manager;
  - Tailgate or allow tailgating through any secure access door;
  - Deliberately hold open a controlled access door by wedging, latching or placing an item against it.
- Employees must:
  - Promptly report any problems relating to access controls to the ICT Director
  - Accompany visitors that are in their care at all times, and not allow them to enter any unauthorised location;
  - Immediately report to the ICT Director and challenge, if confident and safe to do so, any person who is suspected of being in an area that they are not authorised to be in.

INFORMATION BACKUPS

- ICT Director must ensure that:
  - Full back-ups of all software applications and electronic files are completed every 24 hours and retained for 7 days;
  - Additional full back-ups are completed and retained (and destroyed) as required to satisfy relevant contractual, legal and business continuity requirements;
  - All back-ups are protected with an appropriate level of encryption;
  - All back-ups are held in a ISO 27001-certified storage facility;
  - The effectiveness of the back-up process is tested at least once a year by restoring an appropriate sample size of retained backups.

TectoGroup
Unit 2 Spinney View,
Round Spinney Ind Est
Northampton NN3 8RF
T 01604 961 961
E info@tecto.co.uk
W www.tecto.co.uk
Registered in England & Wales No: 07923637

PAPER DOCUMENTS

- Paper documents must be retained (and destroyed) as required to satisfy relevant contractual, legal and business continuity requirements;
- All paper documents must be machine shredded prior to disposal.

USE OF SUPPLIERS

- No supplier should be used to provide services involving the storage, processing, review, access or organisation of Tecto's information without the authorisation of ICT Director.
- No supplier should be used to provide services involving the storage, processing, review, access or organisation of any supplier's, customer's or any other third party's information without the authorisation of ICT Director.

SERVICES TO CUSTOMERS

- No services should be provided to customers that require Tecto to process, review, access, or organise any information provided by
  the customer or on behalf of the customer, that are not covered within Tecto's current Terms and Conditions without the authorisation
  of ICT Director The implementation of this policy is fundamental to the success of Tecto's business, and must be supported and
  adhered to by all employees.

Signed on behalf of Tecto Ltd: Ben Calder
Position: Director
Date: December 2024

TectoGroup
Unit 2 Spinney View,
Round Spinney Ind Est
Northampton NN3 8RF

T 01604 961 961
E info@tecto.co.uk
W www.tecto.co.uk

Registered in England & Wales No: 07923637