IT Security Policy

Introduction

The continued confidentiality, integrity and availability of information systems underpin the operations of CTS Toner Supplies Ltd. A failure to secure information systems would jeopardise the ability of CTS Toner Supplies Ltd to fulfil its day to day operations in the intended manner and would have a greater long-term impact through the consequential risk of financial or reputational loss.

This Electronic Information Systems Security policy provide the guiding principles and responsibilities off all members of CTS Toner Supplies to safeguard its information systems. Other supporting company policies, procedures and guidelines will give greater detail on specific subject areas.

CTS Toner Supplies' are commitment to deliver a successful implementation of Information Security Management but this will only be possible if all members of CTS Toner Supplies are aware of, and carry out their own personal responsibilities.

Purpose of this Policy

The intention of this policy is to:

- Ensure that the information systems that CTS Toner Supplies manage are protected from security threats and to mitigate risks that cannot be directly countered.
- Ensure that all members of the team are aware of and are able to comply with relevant UK and EU legislation
- Ensure that all users are aware of and understand their personal responsibilities to protect the confidentiality and integrity of the data that they access
- Ensure that all users are aware of and are able to comply with this policy and other supporting policies
- Safeguard the reputation of CTS Toner Supplies by ensuring its ability to meet its legal obligation and to protect from liability or damage through misuse of its IT facilities
- Ensure timely review of policy and procedure in response to feedback, legislation and other factors to improve ongoing security.

Scope

This Information Systems Security Policy applies to all members of staff at CTS Toner Supplies and all third parties who interact with CTS Toner Supplies information, and all the systems used to store or process it.

Awareness and Communication

All authorised users will be informed of the policy and of supporting policies and guidelines when their account is issued. Updates to guidance will be publicised internally.

Definitions

CTS Toner Supplies data includes all data elements that are owned or licenced by the organisation or any information processed by CTS Toner Supplies on behalf of a third party.

Information Security Principles

The following principles provide a framework for the security and management of CTS Toner Supplies' information and information systems.

1) Information should be in accordance with legislation, regulatory or contractual requirements that might increase the sensitivity of the information and security requirements.
2) Senior Managers are responsible for ensuring that data is treated in line with appropriate procedures and systems in place. Where personal data is stored, appropriate consent for storage and processing must be gathered and recorded.
3) All individuals covered by the scope of this policy must handle information appropriately in accordance with its classification level.
4) Information should be only available to those with a legitimate need for access.
5) Information will be protected against unauthorised access and processing
6) Information will be protected against loss and corruption
7) Information will be disposed of securely and in a timely manner with measures appropriate for its classification
8) Breaches of policy must be reported by anyone aware of the breach in a timely manner.

Legal and regulatory obligations

CTS Toner Supplies staff must adhere to all current UK and EU legislation as well as regulatory and contractual requirements.

Information Classification

The following provides a summary of the Information Classification levels which are part of the information security principles.

Category – Highly Restricted
Description

- Highly confidential information whose inappropriate disclosure would be likely to cause serious damage or distress to individuals and/or constitute unfair/unlawful processing of "sensitive personal data" under the Data Protection Act/GDPR and/or
- Seriously damage CTS Toner Supplies' interests and reputation; and/or significantly threaten the security/safety of the organisation staff.

Examples

- Sensitive personal data relating to identifiable living individuals
- Bank details and PAYE details of staff
- Bank details of customers/suppliers
- Non-public information that facilitates protection of individuals' safety or security of key functions and assets e.g. network passwords and access codes for higher risk areas.

Category – Restricted
Description

- Confidential information whose inappropriate disclosure would be likely to cause a negative impact on individuals and/or constitute unfair/unlawful processing of "personal data" under the Data Protection Act/GDPR and/or damage CTS Toner Supplies commercial interests
- And/or have some negative impact on the organisations reputation

Examples

- Personal data relating to identifiable living individuals

- Staff contact details.
- Customer contact details.

Category – Internal Use
Description

- Information not considered being public which should be shared only
- Internal but would not cause substantive damage to the organisation and or individuals if disclose

Examples

- Non-confidential internal correspondence e.g. routine administration such as order placement with end users addresses
- Internal policies and procedures

Compliance and Incident notification

It is vital that all users of information systems at CTS Toner Supplies comply with the information security policy. Any breach of information security is a serious matter and could lead to the potential loss of confidentiality, integrity or availability of personal or other confidential data. Such a loss may result in criminal or civil action against CTS Toner Supplies and the loss of business and financial penalties.

Any actual or suspected breach of this policy must be notified to the Commercial Manager who is responsible for IT security at the earliest possible opportunity. All security incidents will be investigated, and consequent actions may follow in line with this policy and any other relevant policies.

The Operations manager must be also informed of any breach found to affect personal data in keeping with the companies GDPR policy.

Responsibilities

Individuals

Individuals must adhere to the Acceptable use policy in the staff handbook and follow relevant supporting guidance. An individual should only access systems and information that they know they have a legitimate right to and not knowingly attempt to gain illegitimate access to other information. Individuals must not aid or allow access for other individuals in attempts to gain illegitimate access to data either. In particular, individuals should adhere to the information security “do’s and don’ts” outlined in the table below.

Do	*Do Not*
Use a strong password and change it if you think it may have been compromised	Give your password to anyone
Report any loss or suspected loss of data	use your password for any other account
Be on guard for fake emails or phone calls requesting confidential information – report anything suspicious to the Commercial Manager	Open any suspicious documents or links
Keep software up to date and use antivirus on all possible devices	Undermine the security of CTS systems
Be mindful of risks using public Wi-Fi, computers or personal devices	Provide access to CTS systems to unauthorised personnel
Ensure CTS data is only stored on our secure S; drive and Cloud based system.	Copy confidential CTS information without permission and avoid using computer desktops for storage
Password protect and encrypt your personally owned devices	Leave your computers and/or phones unlocked.

CTS Toner Supplies' Senior Managers are to understand the full breadth of the information they are responsible for and classify it in line with the information security principles listed above.
Ensure members of staff who maintain information or process data are aware of any additional requirements that may be required to safeguard data above and beyond normal user data.

Data Custodians

Data custodians are responsible for the information systems that hold data and are typically system administrators. They must:

- Ensure that the physical and network security of systems is maintained
- Ensure that the systems they maintain are suitably configured, maintained and developed
- Ensure that the data is appropriately stored and backed up.
- Ensure that appropriate access controls are in place to meet legislative requirements
- Understand and document risks, take suitable steps to mitigate and ensure that these are understood by members of staff.
- Document operational procedures and responsibilities of staff
- Publish procedures for users of the systems to allow secure access and usage
- Ensure that systems are compliant with legal and other contractual requirements.

Commercial Manager (responsible for IT)

The Commercial Manager is responsible to provide specialist advice to all members of the team with the assistance from our external IT company – Initial IT.
Together they will advise on appropriate security measures for any new system types that are introduced.

CTS Toner Supplies Systems used

ECI Horizon (sales and accounts back office system)

Our ECI Software system allows us to store, search, update, remove and delete data. Being able to do this means our software allows us to follow our internal data policies which are a key part of complying with the GDPR.
ECI relies on proprietary and third party data security protection tools and technology designed to help keep data secure. Those include secure delivery of application along with application/domain level security to prevent unauthorised access and other that we determine appropriate from time to time.

Office 365

CTS Toner Supplies use Office 365 as it allows us to own and control our data. They have implemented multiple layers of physical security such as biometric readers, motion sensors, 24 hour secured access and security breach alarms. They enable encryption of data both at rest and via the network as it is transmitted between a data centre and the user. We are confident that Office 365 don't mine or access our data for advertising purposes and they only use our data to provide the service that we pay for. Data is regularly backed up and they enforce "hard" passwords to increase security of our data. Office 365 contractually commit to their promises ensuring excellent data protection.

Internal Audit

Internal audit will ensure that suitable reviews take place of the processes and data classifications.

Mr Steve Clayton
Managing Director