Data Storage and Transfer Policy

Employees at Company Entag Communication are given a variety of resources to do their jobs efficiently and effectively. But it's important that these resources are carefully guarded.

Storing, transferring and sharing company information comes with risks. It can result in data breaches (in which company data is released to people outside of the organization or employees of the organization who haven't been granted access to it), data theft (in which hackers steal information for financial gain or to gather intelligence) and misplaced data (in which original files become lost or unavailable).

The purpose of this policy is to ensure that data is kept available only to current employees of Company Entag Communication who have been pre-approved to possess it.

Data Classification Policy

All data managed by Entag Communication's will be given a data classification policy. This will protect information and enforce document control practices.

The classifications are:

Restricted Data: Data classified as restricted when the unaurthorised disclosure, alternation or destruction of that data could cause a significant level of risk to Entag Communications or customers. High level of security controls will be applied to restricted data

Private Data: Data classified as Private when the unaurthorised disclosure, alternation or destruction of that data would result in little or no risk to Entag Communications or customers. By default, all of Entag's information should be classified as private data. A reasonable level of security control will be applied to Private data.

Public Data: Data classified as Public when the unaurthosised disclosure, alternation or destruction of data would result in little or no risk to Entag or its customers. Examples of Public Data include press releases, advertising material or publications by Entag. Little or no controls are required to protect the confidentiality of Public Data, some level of control is required to prevent unauthorized modification or destruction of Public Data.

Calculating Data Classification

SECURITY OBJECTIVE	LOW	MODERATE	HIGH
CONFIDENTIALITY PRESERVING AUTHORIZED RESTRICTIONS ON INFORMATION ACCESS AND DISCLOSURE, INCLUDING MEANS FOR PROTECTING PERSONAL PRIVACY AND PROPRIETARY INFORMATION.	The unauthorised disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organisational assets, or individuals.	The unauthorised disclosure of information could be expected to have a **serious** adverse effect on organisational operations, organisational assets, or individuals.	The unauthorised disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organisational operations, organisational assets, or individuals.
INTEGRITY GUARDING AGAINST IMPROPER INFORMATION MODIFICATION OR DESTRUCTION, AND INCLUDES ENSURING INFORMATION NON-REPUDIATION AND AUTHENTICITY.	The unauthorised modification or destruction of information could be expected to have a **limited** adverse effect on organisational operations, organisational assets, or individuals.	The unauthorised modification or destruction of information could be expected to have a **serious** adverse effect on organisational operations, organisational assets, or individuals.	The unauthorised modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organisational operations, organisational assets, or individuals.
AVAILABILITY ENSURING TIMELY AND RELIABLE ACCESS TO	The disruption of access to or use of information or an information system could	The disruption of access to or use of information or an information system could	The disruption of access to or use of information or an information system could

AND USE OF INFORMATION.	be expected to have a **limited** adverse effect on organisational operations, organisational assets, or individuals.	be expected to have a **serious** adverse effect on organizational operations, organisational assets, or individuals.	be expected to have a **severe or catastrophic** adverse effect on organisational operations, organisational assets, or individuals.

Email

All data sent over email (as an attachment or in an email text) should be considered sensitive and protected as such. Never send work documents or information to someone outside of the company unless it has been cleared by a manager. *This includes forwarding company emails to your own personal email account.*

Note: Not all users within Company Entag Communication have access to the same information. Before sending data or files to a co-worker in an email, check with your manager to be sure the recipient is allowed to have access to it.

Cloud storage and Cloud Applications

We appreciate that workers may sometimes need access to work outside of the office from home, mobile devices or company equipment on the road. However, *work information should never be stored or shared to personal cloud accounts or applications, such as iCloud, Google Drive, Box, Dropbox, Microsoft OneDrive, etc.*

Should you need to store or backup data online, IT has approved the following services for doing so:

- Box (within Entag Communications tenancy)
- OneDrive for Business (within Entag Communication office 365 tenancy)

If you would like guidance on how to use these services, IT would be happy to assist. And if you have any questions on whether a service is appropriate to use, ask IT *before* using it.

Physical storage devices

Storing work data on physical devices, including but not limited to USB drives, memory cards, CD or external hard drives, must be pre-approved by IT.

- Employees of Company Entag Communication must only use devices provided by the company unless otherwise given permission.
- NEVER use or even plug in a USB drive that you have found or been given as a promotional item. These devices may contain hidden malware or viruses, if you wish to use these devices please have IT approve the devices beforehand
- Lost or stolen devices must be reported to IT and a manager immediately to help ensure their safe return and prevent a data leak.

Social media for work data

Work data including customer information must never be shared over social media accounts such as Facebook, LinkedIn, Google Plus, etc.

If you have any concerns, please contact IT or management for clarification.

Encryption

While encrypting data may not prevent a data breach, it can help ensure that if information falls into the wrong hands it can't be read or used.

Company Entag Communication requires the following types of information to be encrypted: All devices which access customer data must have encryption enabled. All backup services must also encrypt all data. If information is required to be encrypted, it must be protected by a strong password and should never be copied or shared in a way that would make it available outside of the encryption process.