Comply Direct exists to lead, inspire, and educate to positively impact society and the environment. In the day-to-day operation of its business, the company has access to - and is required to store - data and information relating interested parties. These 'interested parties' include, but are not limited to – suppliers, customers, partners, sub-contractors, company visitors and any and all persons with access to information or devices for any reason.

Comply Direct is committed to preserving the confidentiality, integrity and availability of information. All employees, partners, and suppliers have a responsibility to adhere to this Information Security (IS) policy at all times.

Acceptable use

Access

In order to perform their job function, supply agreement, or partnership responsibilities, all parties have a requirement for some level of access to the systems used by Comply Direct. The level of access granted is appropriate to ensure all tasks/responsibilities can be completed.

Use and monitoring of systems and resources

All parties have a responsibility to use the systems, resources and assets provided by Comply Direct in an appropriate manner and only for a legitimate business purpose. All systems, resources and assets provided by Comply Direct remain the property of Comply Direct.

For the purposes of this IS Policy, systems, resources and assets is defined as but not limited to:

- desktop and laptop computers
- desktop phones
- removeable media (such as USB drives and portable hard drives)
- any other physical hardware provided by Comply Direct
- licences for applications made available through employment, supply to, or partnership with Comply Direct and any user accounts associated with these licences/applications

There should be no expectation of privacy for any information stored or transferred on any system, resource, or asset provided by Comply Direct - with the exception of private and/or sensitive information, which will be handled securely in line with the company's GDPR and privacy policies.

Comply Direct and all its parties have a responsibility to monitor and maintain the systems and resources provided and ensure that they remain fit for purpose. Any concerns should be raised with your point of contact.

Installing and updating software

All parties should avoid updating or installing software that may impact information security without first checking with IT staff. Software should only be installed from verified/trusted/known publishers and from known/reputable sources (for example, Microsoft apps should only be downloaded from Microsoft, and not a third-party website). Parties should be aware that vulnerabilities in software can be introduced intentionally (malicious software [malware]) or unintentionally (a bug). Reputable software publishers will work to address any vulnerabilities in their software by periodically releasing updates or patches. Software should have automatic updates enabled where possible to take advantage of this.

Confidential data

It is the responsibility of Comply Direct to define the meaning of confidential data. This has been determined as follows:

- Employee information including but not limited to, personal data, sensitive personal data, and criminal record data (as defined in the Data Protection and GDPR Policy)
- Customer, supplier, and partner information including but not limited to, communications, contact details, data submissions, and data files
- Company information including but not limited to, financial information, pricing structures and management direction

Consideration should be given to any new data or information as to whether it meets the definition of confidential data.

Handling confidential data

All confidential data should be handled securely and not shared with any third parties without prior consent from Comply Direct.

Any need for an individual to handle confidential data outside the functions outlined in their job description, supply agreement, or partnership responsibilities should be discussed with their line manager or senior management, or otherwise point of contact at Comply Direct.

Confidentiality and non-disclosure agreements may be used to protect confidential information.

Network Access

All devices connected to the internet should be secured with a password, and – where possible - setup with antivirus software and a firewall and periodically scanned. This includes personal mobile devices.

Any device containing company information, and all gateway network equipment (e.g. wireless access points, routers, firewalls), should prevent inbound access via the use of the network address translation (NAT) service or a 'deny all' firewall rule. Where inbound access is required, a business case should be created and maintained which will document the reason for such access.

Passwords

Passwords should conform to the guidelines below:

- No password should be saved or transferred as plain text without any additional verification/encryption preventing unauthorised access.
- No password should be written down and stored near the device the password provides access to.
- No password should be saved and stored using browser password storage systems.
- No password should be saved to shared devices under any circumstances.
- If the site/system allows it, a party or individual should provide additional recovery options such as email or text verification codes.
- Passwords should not be duplicated (using the same password for multiple sites/systems).

Making Payments

All parties should have a secure payment process in place. This should include requesting and receiving bank details in appropriate formats (for instance: on company letter headed paper and signed by a director as listed on companies house, or a copy of a blank cheque or paying in slip). Any changes in bank details should be confirmed verbally using a trusted contact number prior to any requested updates.

Relevant training should be conducted for any staff with the authority to input and authorise payments, and at regular intervals, to ensure they are aware and adhering to all cyber and fraud prevention precautions.

Information transfer

All parties should be aware of the different methods of transferring information and the best practises for each to minimise the risk of accidentally leaking information or providing information to an unintended recipient.

Cyber Security Awareness

All individuals should undergo routine cyber security awareness training.

As much as possible, all login accounts that provide access to company information should be secured with an additional layer of authentication (multi-factor authentication).

Electronic

Email

All parties should be aware that phishing emails (emails impersonating another person - often another party) are commonplace. Caution should be used if there is any reason to suspect suspicious activity, particularly if there is an attached file or embedded link. No file or link should be opened or clicked if there is any reason to suspect suspicious activity. It is common for cyber criminals to impersonate senior members of staff - a director or person in a position of financial authority - to try and elicit a sense of importance or urgency along with a request. Where appropriate (particularly if the message is concerning a transfer of money or confidential data) attempts should be made to contact the supposed sender by another method of communication (face-to-face conversation or telephone call). If unsure, parties should highlight any potential phishing emails to IT staff.

The use of a disclaimer highlighting external emails to assist with identifying phishing attempts is recommended.

All parties should take care when replying or forwarding emails to ensure that the content of the email thread is suitable for the intended recipients. Particular care should be taken when using ‘Reply All’, especially if the recipients of the email include both internal and external contacts, and/or if the recipients span numerous departments and job functions.

Telephone

Individuals should consider whether the information to be communicated is suitable for the answering recipient. For inbound calls, individuals should attempt to verify the caller before disclosing any confidential, sensitive or company information.

Cloud file storage (e.g. OneDrive)

A cloud storage solution could be utilised if there is a requirement to share a file with between parties that is difficult to transfer via email because of the file size or type. Care should be taken to ensure

appropriate sharing options/permissions for the file (view, edit, prevent download, etc.) are selected. It is recommended that the file is shared only with specific people and that editing is disabled, a password is set, and downloads are blocked - unless any of this functionality is explicitly required.

Secure file sharing (e.g. WeTransfer)

The use of web hosted file sharing sites such as WeTransfer is not prohibited, but it is recommended that parties explore the use of a cloud storage solution first.

If a web hosted file sharing site is required, parties should first check the security that the site offers and ensure that the site is based in the EU and have a GDPR statement/policy to ensure that they are compliant. Any uncertainty should be highlighted to IT staff.

Physical

There is often a requirement to transfer information physically, either on a USB drive or on a portable device (such as a laptop or mobile phone).

Information carried on portable devices comes with an increased risk of loss or breach, owing to the fact the device has an increased chance of being lost or stolen.

Removable media (portable HDDs and USB drives)

Removable media includes all information storage that be inserted and removed from a system. This includes but is not limited to: CDs, DVDs, USB drives, and portable hard drives.

All removable media containing company information should be encrypted to prevent information breach in the event that the drive is lost or stolen. Removable media should be encrypted using BitLocker. The encryption key is to be obtained from IT staff.

At end of life, all removable media should be formatted to ensure no confidential data can be recovered by any third party. Removable media should be disposed of correctly in line with applicable legislation.

Written information

Individuals should avoid transferring information on paper or other non-electrical medium. This information cannot be protected from unauthorised access should it be lost or stolen. In instances where physical sensitive information is received, it should be stored securely (preferably electronically) if needed and shredded following use.

Devices

All devices that contain or provide access to information should be password protected. Comply Direct operates a ‘clear screen’ policy whereby no information or access to information is left unattended. Devices containing company information should be locked when an individual leaves their desk. Individuals should be aware of the keyboard shortcut to lock a Windows device: Windows Key + L.

All parties should avoid having non-essential business system applications on mobile devices (such as LastPass, Xero & Salesforce). Where an application is required, care should be taken to prevent unauthorised access by signing out of the application when it is not in regular use.

Workstation (desk)

Comply Direct operates a ‘clear desk’ policy. As much as reasonably possible, workstations should be free of confidential and/or sensitive information. Workstations should be tidy and organised to minimise the risk of loss and/or breach of information.

Incident response

Any incident or potential incident of information loss or breach should be highlighted immediately to senior management and IT staff at the soonest possible opportunity.

This communication should include:

- The type of information – confidential or non-confidential
- Details of the information – if known
- Source/cause of the loss or breach – if known
- Any affected parties

All parties should ensure that they are familiar with Comply Directs Business Continuity Policy and, where applicable, the Business Continuity Plan.

Change management

All business changes that may impact information security should be considered in line with this Information Security Policy. In particular, any change should be evaluated to determine if the information affected by the change remains secure and/or if the change introduces any potential of loss or breach of information.

End of contract

At the end of the contract all confidential information stored on any device not owned by Comply Direct must be destroyed or disposed of. No company information acquired during the duration of the contract can be used for any other purpose or shared with third parties. At the end of contract, Comply Direct will retain any information it is legally required to do so, such as compliance and financial information.

Any systems, resources, or assets provided by Comply Direct should be returned to Comply Direct. Any access to systems granted through contract with Comply Direct shall be revoked.