TRUTAC INFORMATION SECURITY POLICY

1 Introduction

1.1 The Company is committed to the highest standards of information security and treats confidentiality and data security extremely seriously. The TruTac resources; systems, networks and the data stored in them are a major asset and it is vital to ensure that they are protected from loss or disruption. Security of the information contained within the IT network is of paramount importance. Additionally, TruTac must protect itself from liability caused by the potential misuse of these resources and loss of confidential data.

1.2 This purpose of this policy is to:

1.2.1 protect against potential breaches of confidentiality;

1.2.2 ensure all our information assets and IT facilities are protected against damage, loss or misuse;

1.2.3 support our Data Protection Policy in ensuring all staff are aware of and comply with UK law and our own procedures applying to the processing of data; and

1.2.4 increase awareness and understanding in the Company of the requirements of information security and the responsibility of staff to protect the confidentiality and integrity of the information that they themselves handle.

1.2.5 The purpose of the Information Security Policy is to take a "common-sense" approach to IT security, but at the same time safeguard the IT network.

1.2.6 The policy does not intend to impose undue restrictions or burdensome process on users and should not make day to day working more difficult.

1.2.7 Staff are requested to refer to aspects of this policy prior to making assumptions in relation to the use of the IT network.

1.2.8 If you have a query about the use of the IT network that's not covered within this policy, please email your query to the IT Department – Chris Williams - Technical Director – Chris.williams@trutac.co.uk

1.2.9 If you have any doubts about the use of an asset on the IT network, please email your query to the IT Department – Chris Williams - Technical Director – Chris.williams@trutac.co.uk

1.2.10 The policy is intended to provide restrictions that allow TruTac to comply with the EU General Data Protection Regulation (GDPR)

Highlighted Elements of the Policy

1.2.11 TruTac computer resources must not be used for the creation, storage, use or distribution of material that may be considered fraudulent, misleading, misrepresentational, harassing, intimidating, defamatory, prejudicial, obscene, profane, sexually explicit, or otherwise illegal or inappropriate.

1.2.12 TruTac systems must not be used to engage in personal, non-work-related activities that could bring TruTac into disrepute.

1.2.13 Users must not attempt to load or connect to personal or third-party computer resources, physical or virtual, that are not a direct asset of TruTac or approved by the TruTac IT Team.

1.2.14 The removal of data from the network on mass storage devices such as USB devices Is not permitted, unless you have an auditable log requesting that you can utilise such devices on and within the TruTac network.

1.2.15 All work undertaken on a day to day basis regardless of department must be stored centrally within the TruTac computer network. The local storing of files (copied onto a laptop / desktop / mobile devices) other than for temporary offline use is not permitted. Local data is not backed up and will be lost should the device fail.

1.3 The IT Department – Chris Williams - Technical Director – Chris.williams@trutac.co.uk is responsible for the monitoring and implementation of this policy. If you have any questions about the content of this policy or other comments you should contact the IT Department – Chris Williams - Technical Director – Chris.williams@trutac.co.uk.

1.4 **Definitions**

TruTac: refers to TruTac Ltd / or its management.

TruTac Computer Resources: means the entire network (connectivity lines such as ADSL and Ethernet), all devices and networks connected to it (including satellite offices, and any other computer related equipment owned or leased by the TruTac. It includes, but is not limited to: -

- Host computers / terminals
- Desktop PC's
- Laptops / handheld devices including tablets
- Virtual Servers – cloud based or physical
- Mail Servers - cloud based or physical
- Web Servers - cloud based or physical
- File Servers - cloud based or physical
- Application Servers - cloud based or physical
- Databases - cloud based or physical
- Software (in house developed or third party supplied)
- Telephone Switches / Virtual Telephone Switches
- IP phones
- Analogue phones
- Bridge phones
- Mobile phones
- USB BitLocker keys
- Printers
- Software data files
- Electronic documents and any communications networks that may be accessed from them.
- All stored / accessible data stored on the network.
- Remote access tokens such as physical Fortinet tokens
- All Cloud based services
- All Cloud based service providers

Computer Equipment: means all equipment within TruTac Computer Resources.

Users: means all employees, agents, contractors, consultants, work placements / experience, apprentice, temporary or fixed term agency staff and any other entity or persons that make use of the TruTac Computer Resources.

Telephone Systems: means all TruTac telephone handsets, headphones, mobile phones, landlines, fax machines and scanners.

Employees and Associates: means all employees, agents, contractors, consultants, work placements / experience, apprentice, temporary or fixed term agency staff and any other entity or persons that make use of the TruTac Computer Resources.

Social Networking Websites: means all social and professional networking websites and accounts visible on the internet publicly or that can be personally restricted; this includes but is not limited to, Facebook, LinkedIn, twitter and snapchat.

2 Scope

2.1 The information covered by the policy includes all written, spoken and electronic information held, used or transmitted by or on behalf of the Company, in whatever media. This includes information held on computer systems, hand-held devices, phones, paper records, and information transmitted orally.

2.2 This policy applies to all staff, which for these purposes includes employees, temporary and agency workers, other contractors, interns and volunteers.

2.3 All staff must be familiar with this policy and comply with its terms.

2.4 This policy supplements the Company's other policies relating to data protection, internet, email and communications, document retention.

2.5 This policy does not form part of any employee's contract of employment and the Company may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted. All users of the TruTac computer resources will have to sign this document to confirm that they understand and will adhere to this policy.

3 General principles

3.1 All Company information must be treated as commercially valuable and be protected from loss, theft, misuse or inappropriate access or disclosure.

3.2 Staff should discuss with line managers the appropriate security arrangements which are appropriate and in place for the type of information they access in the course of their work.

3.3 Staff should ensure they attend any information security training they are invited to unless otherwise agreed by line managers.

3.4 Information is owned by the Company and not by any individual or team.

3.5 Company information must only be used in connection with work being carried out for the Company and not for other commercial or personal purposes.

4 Information management

4.1 Information gathered should not be excessive and should be adequate relevant, accurate and up to date for the purposes for which it is to be used by the Company.

4.2 Information will be kept for no longer than is necessary in accordance with the Company's data retention guidelines. All confidential material that requires disposal must be shredded or, in the case of electronic material, securely destroyed, as soon as the need for its retention has passed.

5 Human resources information

5.1 Given the internal confidentiality of personnel files, access to such information is limited to the Director of Commercial Operations and Marketing. Except as provided in individual roles, other staff are not authorised to access that information.

5.2 Any staff member in a management or supervisory role must keep personnel information confidential.

5.3 Staff may ask to see their personnel files in accordance with the relevant provisions of the Data Protection Act 1998.

6 Access to offices and information

6.1 Office doors must be kept secure at all times and visitors must not be given keys or access codes.

6.2 Documents containing confidential information and equipment displaying confidential information should be positioned in a way to avoid them being viewed by people passing by, e.g. through office windows.

6.3 Visitors should be required to sign in at reception, accompanied at all times and never be left alone in areas where they could have access to confidential information.

6.4 Wherever possible, visitors should be seen in meeting rooms. If it is necessary for a member of staff to meet with visitors in an office or other room which contains Company information, then steps should be taken to ensure that no confidential information is visible.

6.5 At the end of each day, or when desks are unoccupied, all paper documents, backup systems and devices containing confidential information must be securely locked away.

6.6 Customer payment information should not be disclosed to any staff member who does not have the authority to view and or handle that information. No attempt should be made by any staff member that does not have the authority to do so, unless a clear audit trail exists where that staff member has been given clear authority and dispensation by their / an appropriate line manager.

6.7 The recording of customer payment information outside of dedicated transaction systems is prohibited. Information pertinent to customer payments (such as debit / credit card information) should NEVER be recorded or written down outside of these systems. Failure to comply to the safeguarding of financial data could invoke the Company's disciplinary process.

7 Computers and IT

7.1 Use password protection and encryption where available on Company systems to maintain confidentiality.

7.2 Computers and other electronic devices must be password protected and those passwords must be changed on a regular basis. Passwords should not be written down or given to others. Passwords must never be shared and must be a minimum of 8 characters in length (consisting of letters both upper and lower case and at least one Meta character) and no passwords should contain any offensive and / or derogatory language.

7.3 The Company's computer resources and systems must only contain User IDs for current employees and associates. Users must not divulge any of their passwords; only when requested to do so by a line Manager. Users are responsible for the security of their passwords and should not record it in such a way that someone else could discover or guess it. If you believe somebody else may know your password it is your responsibility to change it. Allowing someone else knowledge of your password is a breach of the Computer Misuse Act 1990.

7.4 The IT Team will periodically test the validity of user account passwords that operate within the network. If your password is deemed to be insecure or does not meet the required standard in relation to characterisation, you will be requested to change it.

7.5 To minimise the risk of accidental loss or disclosure, users of computers and other electronic devices must lock their devices each time they are away from their desk and not leave any company or third party sensitive information on screen where it is visible by any person internal or external to the company, that do not have a right to view such information.

7.6 Confidential information must not be copied onto removable hard drive, CD or DVD or memory stick/ thumb drive without the express permission of the IT Department – Chris Williams - Technical Director – Chris.williams@trutac.co.uk and even then it must be encrypted. Data copied onto any of these devices should be deleted as soon as possible and stored on the Company's computer network in order for it to be backed up.

7.7 Removal of data from the network on mass storage devices such as USB devices and portable NAS devices is not permitted, unless you have an auditable log requesting that you can utilise such devices on and within the TruTac network. Invariably this auditable log must include a service ticket reference (when a ticket request was logged to the IT Service Desk as part of the original request) and include agreement from your line manager. If you have been granted the ability to copy information from the network the USB device / Portable NAS device must be supplied by the TruTac IT Team. A Personal USB / NAS device must NOT be utilised.

7.8 All electronic data must be securely backed up at the end of each working day. All work undertaken on a day to day basis regardless of department must be stored centrally within the TruTac computer network. The local storing of files (copied onto a laptop / desktop / mobile devices) other than for temporary offline use is not permitted. Local data is not backed up and will be lost should the device fail. Laptop / desktop / mobile machines and similar devices are not individually backed up to the

TruTac IT network, meaning that in the event of a device failure files stored locally on these devices will NOT be retrievable.

7.9 Staff should ensure they do not introduce viruses or malicious code on to Company systems. Software should not be installed or downloaded from the internet without it first being virus checked. Staff should contact the IT Department – Chris Williams - Technical Director – Chris.williams@trutac.co.uk for guidance on appropriate steps to be taken to ensure compliance.

8 Communications and transfer

8.1 Staff should be careful about maintaining confidentiality when speaking in public places.

8.2 Confidential information should be marked 'confidential' and circulated only to those who need to know the information in the course of their work for the Company.

8.3 Confidential information must not be removed from the Company's offices without permission from the IT Department – Chris Williams - Technical Director – Chris.williams@trutac.co.uk and / or Terry Ramsey – Terry.ramsey@trutac.co.uk except where that removal is temporary and necessary.

8.4 In the limited circumstances when confidential information is permitted to be removed from the Company's offices, all reasonable steps must be taken to ensure that the integrity of the information and confidentiality are maintained. Staff must ensure that confidential information is:

8.4.1 not transported in see-through or other un-secured bags or cases;

8.4.2 not read in public places (e.g. waiting rooms, cafes, trains); and

8.4.3 not left unattended or in any place where it is at risk (e.g. in conference rooms, car boots, cafes).

8.5 Postal, document exchange (DX), fax and email addresses and numbers should be checked and verified before information is sent to them. Particular care should be taken with email addresses where auto-complete features may have inserted incorrect addresses.

8.6 All sensitive or particularly confidential information should be encrypted before being sent by email, or be sent by tracked DX or recorded delivery.

8.7 The printing of information must only be done so when the requirement dictates, as much information as possible should be shared digitally within and across the TruTac IT network. Reference should be made to network links regarding where information is stored, rather than driving an "attachment culture" within TruTac. The printing of personal information not connected with the company or its business is prohibited. Confidential client information should not be printed and or displayed on desks without adequate due care and attention undertaken in order to protect that information.

9 Working at customer's sites

9.1 Devices device must be shut down at the end of each individual customer engagement if each customer engagement is geographically different. The device must not be powered up whilst the device is in transit.

9.2 Information available on the mobile device must only be applicable to that customer engagement at that time. Other customer details must not be shown, discussed, disclosed that are not relevant to that specific customer engagement.

9.3 Specific customer information must be searched for and then displayed to the customer. A search of data on the mobile device must not be undertaken in view of the customer in case other customer information is mistakenly disclosed.

9.4 When in a public place you must be aware of unintentional disclosure of information, such as members of the public being able to see your mobile devices screen, "shoulder surfing", unintentional verbal disclosure of private information.

9.5 Password information to any applications that are to be used in conjunction with the mobile device must not be recorded on paper and taken with you to your location. **ALL** information **MUST** be retrieved and stored digitally.

9.6 Personal information must not be printed and taken with you to your location. **ALL** information **MUST** be retrieved and stored digitally.

9.7 Encryption keys used to encrypt and boot a managed laptop or tablet device must only be known to the user(s) of the device / the IT Team. The encryption key must not be written down and attached to the managed device. If you are using a device that uses an external USB encryption key, the key must not be left inserted within the device, once the device has been booted and is in use.

10 Home working and Remote Access

10.1 Staff should not take confidential or other information home without the permission of the IT Department – Chris Williams - Technical Director – Chris.williams@trutac.co.uk and / or Terry Ramsey – Terry.ramsey@trutac.co.uk and only do so where satisfied appropriate technical and practical measures are in place within the home to maintain the continued security and confidentiality of that information.

10.2 In the limited circumstances in which staff are permitted to take Company information home, staff must ensure that:

10.2.1 confidential information must be kept in a secure and locked environment where it cannot be accessed by family members or visitors; and

10.2.2 all confidential material that requires disposal must be shredded or, in the case of electronic material, securely destroyed, as soon as any need for its retention has passed.

10.3 Staff should not store confidential information on home computers (PCs, laptops or tablets).

10.4 Users working from home be it on a permanent or ad-hoc basis must secure their passwords at all times. Passwords should not be written down or recorded in such a way so that they are on display or are known to family members or non TruTac employees. You should never share you specific IT credentials with other members of your Team or other employees unless specifically requested to do so by your line manager.

Remote access

10.5 Remote access onto the corporate network is granted via the IT Support Team upon receipt of a ticket logged via the Service Desk portal. The ticket must be logged on your behalf by your Line Manager.

10.6 If you are working from home on an **unmanaged** computer device, you will NOT be permitted to connect your device via VPN to the TruTac corporate IT network.

10.7 If you are working from home / in the field on a **managed** device, your access onto the corporate network must be via the prescribed and current authorised VPN method.

10.8 Attempting to connect an unmanaged device / managed device to the TruTac corporate IT network could result in disciplinary action if the former is attempted and the later is attempted outside of the pre-prescribed method.

10.9 All **user to user** communication must be conducted through the corporate email server / realm and to mailboxes tied to the **trutac.co.uk** email domain. User to user communication via any form of "hotmail" or cloud based email services when conducting TruTac business and exchanging corporate information is strictly prohibited.

10.10 Users working from home be it on a permanent or ad-hoc basis must secure their Passwords at all times. Passwords should not be written down or recorded in such a way so that they are on display or are known to family members or non TruTac employees. You should never share you specific IT credentials with other members of your Team / TruTac employees unless specifically requested to do so by your line manager.

Computer Equipment

10.11 TruTac Computer Resources supplied to Users remains the property of the TruTac at all times, as does anything created, stored, sent or received using those resources.

10.12 The TruTac Computer Resources are supplied configured and ready for operational use, and Users must not change, attempt to change or disable any settings on TruTac Computer Resources unless instructed to do so, or where your designated job function requires you to do so.

10.13 Non-work-related software is not permitted to be installed onto any TruTac Computer Resource and includes but is not limited to mobile telephones. Any additional work-related software should be requested via the IT Service Desk and logged as a support request for authorisation by the IT Team via the Service Desk portal.

10.14 Users must lock their computers each time they are away from their desk and not leave any TruTac or Third Party sensitive information on screen where it is visible by any person internal or external to TruTac, that do not have a right to view such information.

10.15 Any computer equipment supplied by TruTac which is lost or stolen must be reported to your line Manager immediately. Line Managers must inform the IT Team by calling the designated support number and by logging a support ticket via the IT Service Desk so that account information on physical devices can be remotely wiped / the appropriate action taken to mitigate risks as a consequence.

10.16 All mobile devices should be secured at all times in protective casing provided. Physical damage to mobile devices must be reported to your line manager. Consistent lack of care / damage to mobile devices may result in disciplinary action.

10.17 If you have been supplied a TruTac managed device (tablet or laptop) , you may also be using this device when working in the field, or from a different geographical location, other than the main TruTac office (s). In both instances the following must be adhered to:

Internal use

10.18 Where devices are to be used for internal use only, an appropriate docking station, mouse, keyboard, stand will be provided to ensure compliance with the latest health and safety regulations.

Devices that have been provided for external use

10.19 Are supplied with a carry sleeve / case in order to protect the device

10.20 Are supplied with a physical portable keyboard.

10.21 Are supplied with an appropriate travel adaptor to power the device.

10.22 Are supplied with either an internal SIM within the device, or an external dongle SIM in order to make an Internet connection.

10.23 The external dongle SIM must be stored separately from the device whilst in transit

10.24 The device whilst in transit must not be displayed or be on show.

10.25 The device must be properly secured whilst in transit to avoid damage to the device.

General operation of the device whilst in the field

10.26 The device must be shut down at the end of each individual customer engagement if each customer engagement is geographically different. The device must not be powered up whilst the device is in transit.

10.27 Information available on the mobile device must only be applicable to that customer engagement at that time. Other customer details must not be shown, discussed, disclosed that are not relevant to that specific customer engagement.

10.28 Specific customer information must be searched for and then displayed to the customer. A search of data on the mobile device must not be undertaken in view of the customer in case other customer information is mistakenly disclosed.

10.29 When in a public place you must be aware of unintentional disclosure of information, such as members of the public being able to see your mobile devices screen, “shoulder surfing”, unintentional verbal disclosure of private information.

10.30 You must ensure that whilst using the device you maintain the correct posture for comfortable use of the device.

10.31 Password information to any applications that are to be used in conjunction with the mobile device must not be recorded on paper and taken with you to your location. **ALL** information **MUST** be retrieved and stored digitally.

10.32 Personal information must not be printed and taken with you to your location. **ALL** information **MUST** be retrieved and stored digitally.

10.33 Encryption keys used to encrypt and boot a managed laptop or tablet device must only be known to the user(s) of the device / the IT Team.

10.34 The encryption key must not be written down and attached to the managed device. If you are using a device that uses an external USB encryption key, the key must not be left inserted within the device, once the device has been booted and is in use.

11 Transfer to third parties

11.1 Third parties should only be used to process Company information in circumstances where written agreements are in place ensuring that those service providers offer appropriate confidentiality, information security and data protection undertakings.

11.2 Staff involved in setting up new arrangements with third parties or altering existing arrangements should consult the for more information.

E-mail / Instant Messaging, Skype for Business, TeamViewer, Zoho or similar

11.3 E-mail and other forms of electronic communication, including Instant Messaging, SMS text services and collaborative online document sharing capabilities have the same legal and business standing as any other form of written communication and therefore they must be treated with the same care, attention and diligence.

11.4 Where Skype For Business or other application or screen sharing tool is utilised for ad-hoc meetings, between individual or group Users, appropriate behaviour is expected at all times, in line with courtesy and behaviour to that of physical face to face meetings.

Users must not

11.5 Forward e-mail to anyone external to TruTac other than in connection with legitimate business activity.

11.6 Bring TruTac into disrepute by sending unwarranted emails that others could deem as unsolicited email.

11.7 Initiate or participate in chain emails / chain Lync / Team messaging; any such e-mails or Lync messages received must be notified to your line manager. The line manager must report such instances to the IT Service Desk by logging a ticket through the Service Desk portal.

11.8 Interfere with any e-mail branding or signature applied by TruTac to their e-mail account.

11.9 Download personal e-mails or use different software or add additional e-mail accounts to the designated TruTac e-mail system or forward any emails (including attachments) received via the TruTac e-mail account to their own personal e-mail account. All incoming attachments that are zipped (compressed) will be checked for viruses. If applicable the intended recipient may be required to provide an explanation of what the file is for.

Users must:

11.10 Regularly review all e-mails posted to their TruTac e-mail account and any other TruTac account(s) they have access to.

11.11 Ensure all e-mails are responded to in a timely manner and sorted appropriately.

11.12 Use the same care in drafting e-mails and other electronic documents as they would any other form of business communication. All language should be to a professional business standard without “over familiarity”, “slang” or what could be deemed as “text” language.

11.13 Be aware of the commercial ramifications of all e-mails sent and received.

11.14 Ensure that e-mails using designated group listings from the TruTac e-mail distribution lists are work related only and have a clear defined business purpose.

11.15 Where applicable email links to documents that are stored on the network, rather than send bulky attachments via email. This will reduce email traffic and help Users to manage the size of individual mailboxes.

11.16 TruTac will monitor storage usage and request action to be taken when your mailbox is about to reach full capacity or has reached full capacity. Where applicable the sending and receiving of large attachments should be facilitated via the IT Team. The use of Dropbox is allowable, only after consultation and permission is sought via the IT Team.

11.17 A User should not bring TruTac into disrepute by sending unwarranted messages to individual or groups of internal Lync Users where that message is without a business need, necessity or requirement. The same professional judgement, care and attention needs to be considered to that of emails when composing and sending Lync messages.

Office 365 accounts

11.18 Staff utilising Office 365 accounts should not attempt to set up a copy, duplicate or auto forward function within the TruTac Office 365 realm to an additional private email account linked to that staff member. Any such functions setup in this manner need agreement from your line manager with the configuration being undertaken by the IT Team. A clear audit trail (Service Ticket) must exist for exceptions such as these. Failure to follow this process could lead to the TruTac disciplinary process being invoked.

11.19 Should you consistently need to access your Office 365 profile outside of core business hours (but you do not have a managed device in which to do so), please speak with your line manager regarding your requirements.

12 Overseas transfer

12.1 There are restrictions on international transfers of personal data. Staff must not transfer personal data internationally at all OR outside the EEA (which includes the EU, Iceland, Liechtenstein and Norway).

13 Reporting breaches

13.1 All staff have an obligation to report actual or potential data protection compliance failures to the IT Department – Chris Williams - Technical Director – Chris.williams@trutac.co.uk and / or Terry Ramsey – Terry.ramsey@trutac.co.uk. This allows the Company to:

13.1.1 investigate the failure and take remedial steps if necessary; and

13.1.2 make any applicable notifications.

14 Consequences of failing to comply

14.1 The Company takes compliance with this policy very seriously. Failure to comply puts both staff and the Company at risk. The importance of this policy means that failure to comply with any requirement may lead to disciplinary action, which may result in dismissal.

14.2 Staff with any questions or concerns about anything in this policy should not hesitate to contact the IT Department – Chris Williams - Technical Director – Chris.williams@trutac.co.uk and / or Terry Ramsey – Terry.ramsey@trutac.co.uk.