INTEGRATED SYSTEM POLICY

INFORMATION SECURITY STATEMENT

1. SCOPE

1.1. X-Net recognises individuals and organisations with whom they conduct business with value their privacy, and reasonably expect X-Net will take steps in protecting information held about them and their businesses.

1.2. Customer information is information which is directly associated with a specific person or business e.g. user's name, address, telephone number and sometimes information about online or network activities etc. The collection of customer information is both necessary and desirable in the conduct of X-Net's business. X-Net is committed to continually improving and protecting the privacy and security of both the individual and their business information encountered whilst conducting business. To prevent the misuse of the individuals or businesses information. Ensuring business continuity, confidentiality and confidence with X-Net.

1.3. The confidentiality, integrity and availability of information, in all its forms are critical to the on-going functioning and good governance of X-Net. Failure to adequately secure information increases the risk of financial and reputational loss from which it may be difficult for X-Net to recover.

2. POLICY STATEMENT

2.1. Protection of Data:

2.1.1. X-Net maintains physical, electronic and procedural safeguards for information collected through and stored within X-Net. This data is retained in accordance with our, P-DR Data Retention Policy. The data is retained and used for the conduct of X-Net's business, including accounting, billing, auditing, administrative, legal purposes, security and payment verification. Appropriate technical and organisational measures are taken to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data. All legislative and regulatory requirements are met in accordance with the Data Protection Act 2018 and General Data Protection Regulation (GDPR).

2.1.2. The Data Protection Officer (DP) will ensure the appropriate technical and organisational measures as mentioned in 2.1.1 are applied at the appropriate level based on the assessed security risk of each area, this should enable:

2.1.2.1. The pseudonymisation and encryption of personal data.

2.1.2.2. The ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services.

2.1.2.3. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

2.1.2.4. Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2.1.3. Where a personal and/or data breach has occurred and is likely to effect the rights and freedoms of individuals effected the DP Officer shall communicate this without delay. Information communicated should at least contain:

2.1.3.1. Name/s and contact details of DP Officer and/or other appointed personnel.

2.1.3.2. Describe the likely consequences of the personal data breach.

2.1.3.3. Describe the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate the possible adverse effects.

2.1.4. Personnel:

2.1.4.1. Information security training is provided on an on-going basis to all personnel and forms part of the induction training for new personnel. Supporting procedures are in place defining security policy with regard to availability of information and information systems, security controls, password controls and software encryption. All breaches of information security, actual or suspected are reported to the Security Working Group (SWG), who is responsible for maintaining the security policy and providing advice and guidance on its implementation. All business managers have a responsibility for the implementation of the policy within their business areas and for adherence by their personnel. It is the responsibility of every miner of personnel to adhere to this policy.

3. COMPLIANCE

3.1. Information security auditing will conduct regular monitoring to enforce compliance with this policy. Any violation of this policy will be investigated and if found to be caused by wilful disregard or negligence, will be treated as a disciplinary offence. All disciplinary proceedings are coordinated.

3.2. X-Net reserves the right to amend this policy at any time and will publish updated versions to all personnel.