XMISSION SECURITY POLICY STATEMENT

As an established and reputable provider of colocation, hosting, email, and connectivity services, XMission is strongly committed to security. XMission's services are designed to offer the security, resources, expertise and performance of a large and geographically diverse hosting provider while maintaining the accessibility, personal relationship, trust, and attention of a smaller, less corporate organization.

Objectives

XMission's objective for managing information security is to ensure business continuity and mitigate risk by preventing and minimizing the impact of security incidents. Therefore, XMission has established policies and procedures (i.e., internal controls) based not only on industry-wide information security forensics but also on the experience and expertise of our talented staff. XMission's Management Team aims to maintain existing known risks at their current low level and ensure that future risks are managed in an equally consistent and professional manner.

Purpose

The intended purpose of the Policy is to protect both XMission and its customers' assets from all threats, whether internal or external, deliberate or accidental. Protection of information is set out in terms of:

- Confidentiality: ensuring only persons who are authorized have access to information.
- Integrity: ensuring the accuracy and completeness of information.
- Availability: ensuring information, associated assets, and systems can be accessed when required by authorized persons.
- Regulatory: abiding by all regulations, laws and codes of practice everywhere XMission operates.

In particular XMission will:

- Ensure that XMission management and employees comply with the requirements of the security policy.
- Minimize the risk of damage to company assets, information, reputation, hardware, software and data.
- Set out clearly the company's policies relating to all aspects of the management of information, hardware, firmware and software. This includes virus control measures as well as password and network security.
- Develop, maintain, test, update, and continually improve upon business continuity plans.
- Set policies and procedures to reduce risks to reasonably acceptable levels. Determining criteria to identify acceptable levels of risk.

The security manager, working closely with the CTO, has direct responsibility for maintaining the Security Policy and providing advice and guidance on its implementation.

All managers are directly responsible for implementing the Security Policy within their business areas, and for adherence by their staff.

It is the responsibility of each member of staff to adhere to the Security Policy.

Pete Ashdown
XMission President