Cyber Security Policy

Cyber Security is concerned with the protection against the criminal or unauthorised use of electronic data. Implementation of appropriate controls can provide the business with basic protection from the most predominant forms of threats associated with the internet.

We are committed to ensuring the protection of all operational systems and data within our own network, alongside reducing the risk introduced by working with suppliers or third parties. The evolving nature of the threat, along with the growth of the business makes it likely that there could be vulnerabilities resulting in insufficient protection to the business.

Aims of the policy

This policy is designed to support the company in reducing its vulnerability to cyber-attack. It sets out our principles and checks regarding cyber security as good practice, and also highlights our responsibilities to suppliers to reduce risk through supply chain assurance.

To address the threat posed to the business through cyber-attack and recommend the use of risk management in order to protect personal or sensitive information & data, we will raise awareness of cyber security throughout the business, and ensure that defences are operated consistently across all areas and technology domains.

To recognise the extent of our exposure to cyber-attack as a business and ensure that systems are developed and maintained to reduce the risk imposed.

Objectives of the policy

1. To assess the risk to the business at present and implement security controls that are proportionate to the business needs.
2. To undertake an assessment of implementation of cyber controls to ensure that all risks across all areas of the business are met.
3. To address the threat to the business by maintaining our ‘Cyber Essentials’ certification and demonstrate to clients that ISS Labour maintains a robust cyber security stance.

In order to reduce the risk of cyber-attack within the business, we will focus on the following critical areas:

i. Information Risk Management

ii. Secure Configuration

iii. Network Security

iv. Managing User Privileges

v. User Education & Awareness

vi. Incident Management

vii. Malware Prevention

viii. Monitoring

ix. Removable Media Controls

x. Home & Mobile Working

There will be a clear and concise framework drawn up to ensure that all ten areas above are phased into the business, and to guarantee the successful demonstration of cyber security across all areas of our business.

To ensure effectiveness in adopting the cyber security principles laid out below we will approve procedures based on a risk-based approach and ensure that our staff recognise the risk and act accordingly.

Principles

a) To understand the importance of culture & environment in which risk management activities are effective.

b) To understand the values of effective risk management approaches.

c) To accept that there will always be uncertainty – risks are not always predictable and cannot always be eradicated.

d) To make all members of staff part of the delivery team when it comes to cyber security. To ensure everyone understands what the business is trying to achieve and to be transparent in our security goals.

e) To ensure the business understands the risks it is taking in regard to cyber security and to identify what areas are important to ISS Labour.

f) To understand that security is a part of every technology decisions within the business.

g) To ensure security is valued by the business and that risk management needs to support business processes rather than just run alongside them.

h) To understand that risk management is a continuous activity and that one-off risk assessments are not effective to the business' security.

Communication, Monitoring and Review

We will ensure that this policy is communicated to all individuals to which it applies, is available to relevant interested parties and is reviewed at least annually for effectiveness.

Gary Beeston
Group Managing Director