

# Cyber Security

## Document Control

Reference: Cyber

Issue No: 1

Issue Date: 25/04/2018

## 1. Purpose

iSAMS Independent Ltd has a commitment to keeping data safe and using proven state of the art technologies. iSAMS Independent Ltd is mindful of the Government Cyber Essentials standard and forms the basis of our approach to security.

This document provides an overview of the Cyber Security Essentials at iSAMS Independent Ltd covering:

- System Configuration
- Firewall
- Email Security
- System User Access
- Patch Management
- Malware Protection

Further information and records are available from the iSAMS Independent Ltd Network Support documentation.

The technologies outlined are current and are upgraded as new releases and advancements are made.

## 2. System Configuration

All iSAMS Independent Ltd's internal systems use Active Directory and are domain joined. This process enforces that a "Group Policy" is applied to each system, effectively configuring it centrally.

Access to all servers is restricted to network administrators.

All users access these servers using their own credentials (no shared credentials)

Any required shared credentials are shared via the use of a Password Manager (LastPass)



### **3. Firewall**

iSAMS Independent Ltd have a Cisco ASA5525X.

The firewall has very rigid access controls – only specified users are allowed access.

iSAMS Independent Ltd has an external consultancy to help us if we have any problems with the Firewall (Lynx Networks)

### **4. Email Security**

iSAMS Independent Ltd utilises Mimecast which is an email security system. This helps our users avoid getting infected with email based malware.

### **5. System/User Access**

iSAMS Independent Ltd operates Active Directory and have full access control lists.

Only network administrators have access to admin tasks.

iSAMS Independent Ltd has a strong password policy which is in line with the NCSC guidelines.

User Access is granted depending on the individual's role. User Access changes as an individual moves role within iSAMS Independent Ltd and is removed once they become a 'leaver'.

### **6. Patch Management**

iSAMS Independent Ltd utilises Group Policy to configure patch management.

Windows Updates are set to install automatically on a weekly basis. Given that the updates are released monthly, this is very fast. This policy applies to all workstations and servers.

Any new threats are assessed as to whether a manual patch is needed and appropriate action is taken.

### **7. Malware Protection**

iSAMS Independent Ltd uses Sophos Anti-Virus across all our workstations and servers.

### **8. Responsibilities**

The iSAMS Independent Ltd Network Manager is responsible for ensuring that iSAMS Independent Ltd maintains the areas outlined in this document.

The iSAMS Independent Ltd Network Manager will also keep records and logs for audit and accountability purposes.



The iSAMS Independent Ltd Network Manager is responsible for ensuring compliance.

### Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue	Head of Service and Operations	25/04/2018

