

# **Information Security Policy**

## **Introduction**

Information and information systems are vitally important to Companies House. Without reliable information and information systems, Companies House would be unable to deliver its services or meet its targets.

Information must be protected in a manner appropriate to its sensitivity, value, and criticality. Security measures are to be used regardless of the media on which information is stored, the systems that process it, or the methods by which it is processed.

## **Scope**

This policy outlines the responsibility that all managers, staff and contractors have in order to ensure the security of Companies House information. It provides a framework of procedures, standards and controls to ensure that all information is maintained securely.

## **Purpose**

The policy sets out the approach taken to manage the confidentiality, integrity and availability of information. This is in order to ensure that all information is properly protected against a variety of threats such as error, fraud, sabotage, terrorism, extortion, industrial espionage, privacy violation, service interruption, theft and natural disaster, whether internal or external, deliberate or accidental.

## **Your Responsibility**

It is the responsibility of all Companies House employees and contractors to report any software malfunctions, security incidents, suspected viruses, faults, weaknesses or threats observed or suspected to the relevant Helpdesk as soon as possible. This will ensure that relevant countermeasures are taken to minimise the impact of the incident and to ensure that recurrence is prevented. If in doubt, talk to your line manager or the Information Security Manager.

Information security requires the participation and support from all staff. All staff will be provided with sufficient training and guidance to allow them to protect and manage Companies House information assets.

## **Further Information**

Staff should familiarise themselves with the full requirements of the various security policies and procedures to ensure compliance. All these policies can be found on the Information Security section of the Intranet or can be obtained in hard copy from IT Security. Breach of the policies might lead to disciplinary action.

If you require any further information please contact IT Security