Loss Prevention Standards – Asset Classes

Security - Computer Equipment

Version: 1.2
Date: 25th April 2025

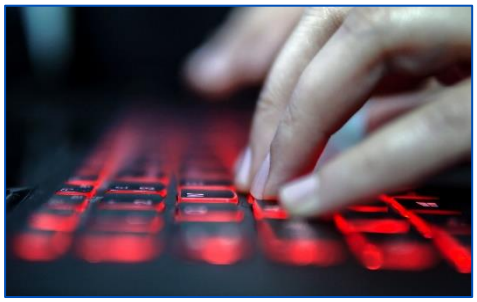
Certain items of computer equipment are generally considered theft-attractive and are often essential to the operations of most businesses.

This Loss Prevention Standard provides guidance on security arrangements for such equipment.

AVIVA

Security - Computer Equipment

Introduction



There are few commercial premises that do not have at least one computer. In most large organisations, computer equipment and their related communication networks are critical to normal operations.

Whilst cyber security has become a significant issue in recent years, thieves can still be attracted by the portability and general anonymity of many items of equipment, such as laptop computers and tablets, and the value of high specification network and/or web servers.

This Loss Prevention Standard outlines the main procedures for assessing and managing security in relation to computer equipment. For specific guidance on cyber security, refer to Aviva's Cyber Loss Prevention Standards.

Risk Assessment

The required security protections should be determined via a security risk assessment, which should include:

- The financial cost of replacing stolen computer equipment, systems or data.
- The anticipated equipment/software replacement times.
- The vulnerability of the premises, systems or data to unauthorised physical or electronic access.
- The effect on business operations:
  - ✓ Direct and indirect business impact.
  - ✓ Reputation and customer confidence.

The risk assessment should be undertaken and reviewed by persons with suitable knowledge of the premises, including occupancy levels, and the key or critical computer equipment and be someone able to make, or influence security funding decisions. The use of a Security Consultant, preferably one registered with the Register of Chartered Security Professionals, and with a speciality in computer and IT security, should be considered where necessary.

The risk assessment should be recorded and routinely reviewed, particularly prior to any significant changes being made to the computer equipment in use at the premises. Responsibility for oversight of any control measures identified in the risk assessment should be delegated to a responsible person.

Managing the Risks

The most effective security protection is generally provided by a range of complementary measures under the following headings.

Important: When reviewing computer equipment-related security measures, businesses should check whether any interested parties such as an insurer or a leasing company, have any specific requirements.

Procedural Security Measures

Considerations include:

- Ensure access is limited to appropriately authorised individuals such as employees and customers and that access is:
  - ✓ Reviewed periodically.
  - ✓ Removed when someone leaves the organisation, or if procedures are not followed.
- Passwords and other procedures should limit individual access to required systems and equipment only.
- Install and maintain up-to-date anti-virus software and internet firewalls.

- Implement strict and clear employee controls on use of the internet, downloading software, use of data encryption and memory sticks, etc.
- Ensure users are aware of the theft risks of leaving equipment unattended in public areas, sections of the workplace or when working away from the premises.
- Ensure users do not leave computer equipment in unattended vehicles.
- Ensure users do not travel with items such as laptops in easily recognisable carrying cases.
- Do not position theft-attractive equipment next to externally accessible glazing.
- Maintain an asset register, i.e. a list of all serial numbers and installed locations of computer equipment.
- Avoid inadvertently advertising the arrival of new equipment, and do not:
  - ✓ Stockpile or store in readily visible locations.
  - ✓ Leave in non-secure or common areas, etc.
- By way of a deterrent, it may be prudent to advertise any security measures that may not otherwise be readily apparent. For example, posting notices that the premises benefit from monitored intruder alarm protection, or equipment marking systems are in use, etc.
- Ensure critical and important computer data is regularly backed-up and copies are maintained off site in a secure location, or appropriate cloud based back-ups are maintained.
- Develop and maintain a Business Continuity Plan (BCP) to support the recovery of your computer systems after any security (or other) incident. This should be:
  - ✓ Maintained up to date, reviewed and revised periodically.
  - ✓ Tested regularly.

Physical Security Measures

Premises. A well-secured perimeter, both in relation to external areas of the building and to specific internal areas within the premises provides significant security protection. Considerations include:

- Building construction and resilience to theft attack.
- Location.
- Ease of access.
- Hours of occupancy.
- Type (theft-attraction) of the computer equipment present.

IT suites and server rooms in particular, often contain concentrations of expensive or critical equipment. Organisations should ensure these rooms are robustly built, sited away from outside walls (ideally on upper floors), not visible from outside of the building, and that good quality doors and locks are fitted.

Refer Aviva Loss Prevention Standard **Server/Comms Rooms** for further guidance.

Security Guarding. At some premises, the values at risk, the business exposure or the effect of a loss to reputation should an incident occur, etc., may require a physical guarding presence, during or outside business hours, or both.

In the United Kingdom, the National Security Inspectorate (NSI) listing is an indicator of full compliance (supported by external auditing) with UK manned guard licensing rules and good security practice, e.g. adherence to recognised British Standards. Membership of the Security Industry Authority Approved Contractors Scheme (ACS) is also indicative of good standards.

Although it may conflict with operational convenience, care should be taken to ensure that guards are suitably protected against duress, i.e. they cannot be forced to unset alarms or unlock doors, etc. This is best completed by stationing guards outside of any building they are guarding and not permitting them to hold keys, codes or un-setting devices for electronic security systems.

Electronic Security Measures

Electronic security devices supplement the primary physical and procedural protections. Options include:

- Access control systems to assist in vetting/controlling persons seeking access to, or within key parts of, the premises.
- Locally or remotely monitored intruder and hold-up alarm systems.
  - ✓ Further guidance is provided in the Aviva Loss Prevention Standard **Intruder and Hold Up Alarms – General Guidance.**
- A locally monitored Video Surveillance System (VSS) which supports the management, monitoring and/or recording of visitors during operational hours.
- An external remotely monitored, detector-activated VSS.
  - ✓ These can be particularly effective outside business hours in detecting potential intruders whilst they are still outside the premises, i.e. before a break-in is attempted or occurs.
  - ✓ The nature of such systems requires careful attention to system design and operating procedures if they are to be effective.
  - ✓ Further guidance is provided in the Aviva Loss Prevention Standard **Video Surveillance Systems – Introduction**.
- A 'smoke' generating security fog device operated by alarm sensors. When activated, these rapidly fill an area with a dense, non-harmful chemical fog which obscures vision, and may prevent potential intruders from clearly seeing theft-attractive items whilst hindering their movement within the premises.
  - ✓ Additional information on this topic is provided by the RISCAuthority via their publication **S07 Security Guidance for Fog Devices** which is available at the RISCAuthority Resource Index.
- A forensic intruder marking system, which when activated, fills a contained environment with a near invisible, non-harmful, uniquely formulated chemical mist, which adheres to the clothes and body of intruders. The police can detect this marking on individuals and trace it back to the registered premises.

Equipment Security Measures

Whilst site-wide procedural, physical and electronic security measures can provide a robust line of defence, security measures applied to specific items of equipment can provide additional security and may provide an effective deterrent to potential thieves.

Options to consider include the following:

- Provide permanent visible marking (etching) of equipment with details of the company name and postcode.
- Provide covert forensic marking.
- Secure equipment to walls or furniture with steel cable ties to hinder removal.
- Secure equipment in an 'entrapment' device bolted/anchored to a floor, wall or desk. This will help prevent easy removal of the equipment or any internal components.
  - ✓ Further guidance is provided in the Loss Prevention Certification Board Standard LPS1214 Specification for testing and classifying physical protection devices for personal computers and similar equipment.
- Use of equipment alarms which emit an audible signal if the equipment is moved or interfered with. These are ideal for alerting nearby individuals to 'walk-in' theft or unauthorised use.
- Use of internet tracing devices which can send a message if a computer is used from an unauthorised location, e.g. after being stolen, which in turn can help establish its current location.

Checklist

A generic **Computer Equipment Checklist** is presented in Appendix 1 which can be tailored to your own organisation.

Specialist Partner Solutions

Aviva Risk Management Solutions can offer access to a wide range of risk management products and services via our network of Specialist Partners who are reputable companies offering agreed discounted rates for Aviva customers.

Electronic Security Services - **Secom**

Security marking - **Selectamark**

For more information please visit: Aviva Risk Management Solutions – Specialist Partners

Sources and Useful Links

- National Security Inspectorate (NSI)
- Security Systems and Alarms Inspection Board (SSAIB)
- British Security Industry Association (BSIA)
- Master Locksmith Association
- Security Industry Authority Approved Contractors Scheme

Note: Whilst UK standards and legislation are referenced in this document, other international standards and legislation should be referenced where applicable.

Additional Information

Relevant Aviva Loss Prevention Standards include:

- **Intruder and Hold Up Alarms – General Guidance**
- **Intruder Alarms European Standard**
- **Locks – Security**
- **Security – Doors, Windows and Other Barriers**
- **Video Surveillance Systems - Introduction**
- **12 Top Tips to Protect Against Cyber Attack**
- **Cyber Essentials Accreditation**
- **Cyber – Incident Response Process**
- **Cyber – Ransomware**
- **Cyber - Respond and Recover**
- **Cyber – The Internet of Things**
- **Cyber - Social Engineering**
- **Business Impact Analysis**
- **Business Continuity Management**
- **Business Continuity Plan – Testing and Maintenance**
- **Managing Change - Property**

To find out more, please visit Aviva Risk Management Solutions or speak to one of our advisors.

Email us at riskadvice@aviva.com or call 0345 366 6666.*

*The cost of calls to 03 prefixed numbers are charged at national call rates (charges may vary dependent on your network provider) and are usually included in inclusive minute plans from landlines and mobiles. For our joint protection, telephone calls may be recorded and/or monitored.

Appendix 1 – Computer Equipment Security Checklist

Location	
Date	
Completed by (name and signature)	

	Computer Equipment Security	Y/N	Comments
1.	Have Business Impact and Security Risk Assessments been undertaken of the current IT/computer security at your premises, including the following? • Local or business history of IT security related events? • The cost of replacing computer equipment, systems or data? • Expected equipment/software replacement times? • Accessibility and vulnerability of premises, systems or data to unauthorised physical or electronic access? • The business impact on your operations: ✓ Reputation and customer confidence? ✓ Loss of computer equipment, systems or data? ✓ Malicious interference with computer equipment, systems or data? • Strength and nature of the building construction, doors, windows and securing mechanisms? • The nature of any other electronic security measures or human presence on site?		
2.	Has any independent or specific crime prevention advice or security requirements been sought from: • The police? • A security consultant? • Your insurer? • Equipment leasing company?		

	Computer Equipment Security Contd.	Y/N	Comments
3.	Do your password rules and other procedures limit employee and customer access to systems and equipment?		
4.	Has anti-virus software been installed and is this up to date?		
5.	Are there clear employee controls on internet usage, downloading software and the use of data encryption?		
6.	Have users been made aware of the theft risks of leaving equipment unattended in public; in unattended vehicles; carrying items in recognisable laptop bags; leaving them in clear line of sight of windows and doors?		
7.	Is an asset register maintained of all serial numbers and the location within the business of computer equipment?		
8.	Is important and critical computer data regularly backed-up and copies maintained off site in a secure location, or appropriate cloud based facility?		
9.	Has a BCP for the IT hardware and systems been prepared? • Is this a live document which is regularly reviewed? • Is this tested?		
10.	Has the location of any IT or server rooms been considered? • Are these visible or accessible from the building exterior? ✓ Are additional measures in place to protect any glazing to the exterior? • Can the room be accessed through a weak vulnerable ceiling/floor above or from a floor below? • Is access to these areas restricted the closer one gets to the room? • Are these rooms locked at all times? • To prevent 'unmanaged open doors', do the doors into the room have automatic closing and latching mechanisms? ✓ Are door wedges prohibited? • Is access to these rooms limited to a named group of individuals?		

	Computer Equipment Security Contd.	Y/N	Comments
11.	Are the premises protected by electronic security systems? • A Video Surveillance system (VSS)? • An access control system? • A remotely monitored intruder alarm system?		
12.	Is the computer equipment hardware 'property-marked'? • Visible marking (etching) of equipment with details of the company name and postcode? • Covert forensic marking?		
13.	Is high value or business critical equipment secured by a proprietary 'entrapment' device? Is this bolted/anchored to a floor, wall or desk to prevent easy removal of equipment or internal components?		
14.	Are the security measures of the IT hardware equipment and software systems considered within a formal Management of Change process? • For new software systems? • For new hardware? ✓ Delivery? ✓ Receipt? ✓ Storage? • For removal of old hardware? • New employees? • Departing employees?		
15.	Are all employees formally trained on your IT policies and security measures, and does this include: • All employees? • Contractors? • Repeat training?		

	Computer Equipment Security Contd.	Y/N	Comments
16.	Are security arrangements and the basis for the risk assessment reviewed following any security issues, local incidents, intrusions or losses etc.? **Note:** If not, you are likely to be at more risk of a repeat incident.		
17.	Additional comments:		

Please Note

This document contains general information and guidance only and may be superseded and/or subject to amendment without further notice. Aviva has no liability to any third parties arising out of ARMS' communications whatsoever (including Loss Prevention Standards), and nor shall any third party rely on them. Other than liability which cannot be excluded by law, Aviva shall not be liable to any person for any indirect, special, consequential or other losses or damages of whatsoever kind arising out of access to, or use of, or reliance on anything contained in ARMS' communications. The document may not cover every risk, exposure or hazard that may arise, and Aviva recommend that you obtain specific advice relevant to the circumstances.

25th April 2025

Version 1.2

ARMSGI1422020