LPCB®

Loss Prevention Standard

LPS 1224: Issue 3.1

Requirements for companies providing secure asset registration services

This standard specifies requirements for asset registration companies providing secure asset registration services designed to support the identification and repatriation of assets when those assets are lost or stolen

bre

CONTENTS **PAGE**

PARTICIPATING ORGANISATIONS

This standard was approved by the LPC Fire and Security Board and Expert Group G.

The following organisations participated in the preparation and review of this standard:

Association of British Insurers
Association of Building Engineers
Association of Chief Police Officers
Association of Insurance Surveyors
Association for Specialist Fire Protection
British Automatic Fire Sprinkler Association
British Security Industry Association
BT
Chief Fire Officers Association
Door & Hardware Federation
Electrical Contractors Association
European Fire Sprinkler Network
FIA
Health & Safety Executive
Home Office
Home Office Scientific Development Branch
Metronet
National Counter Terrorism Support Office
Post Office
Risk Engineering Data Exchange Group
Royal and Sun Alliance
Royal Institution of Chartered Surveyors
Special Services Group

REVISION OF LOSS PREVENTION STANDARDS

Loss Prevention Standards will be revised by issue of revised editions or amendments. Details will be posted on our website at www.redbooklive.com

Technical or other changes which affect the requirements for the approval or certification of the product or service will result in a new issue. Minor or administrative changes (e.g. corrections of spelling and typographical errors, changes to address and copyright details, the addition of notes for clarification etc.) may be made as amendments. (See amendments table on page 47)

The issue number will be given in decimal format with the integer part giving the issue number and the fractional part giving the number of amendments (e.g. Issue 3.2 indicates that the document is at Issue 3 with 2 amendments).

USERS OF LOSS PREVENTION STANDARDS SHOULD ENSURE THAT THEY POSSESS THE LATEST ISSUE AND ALL AMENDMENTS.

FOREWORD

This standard identifies the evaluation and assessment practices undertaken by LPCB for the purposes of approval and listing of secure asset registration services. LPCB listing and approval of products and services is based on evidence acceptable to LPCB:

- that the product or service meets the standard
- that the manufacturer or service provider has staff, processes and systems in place to ensure that the product or service delivered meets the standard

and on:

- periodic audits of the manufacturer or service provider including testing as appropriate
- compliance with the contract for LPCB listing and approval including agreement to rectify faults as appropriate.

Full details of the LPCB scheme for approval and listing of secure asset registration services to this standard are provided in scheme document SD152.

NOTES

Compliance with this LPS does not of itself confer immunity from legal obligations. Users of LPSs should ensure that they possess the latest issue and all amendments.

LPCB welcomes comments of a technical or editorial nature and these should be addressed to "the Technical Director" at enquiries@breglobal.co.uk.

The BRE Trust, a registered charity, owns BRE and BRE Global. BRE Global and LPCB (part of BRE Global) test, assess, certificate and list products and services within the fire and security sectors. For further information on our services please contact BRE Global, Watford, Herts. WD25 9XX or e-mail to enquiries@breglobal.co.uk

Listed products and services appear in the LPCB "List of Approved Products and Services" which may be viewed on our website: www.redbooklive.com or by downloading the LPCB Red Book App from the App Store (for iPhone and iPad), from Google Play (for Android devices) or from the Windows Store (for Windows 8 Phones and Tablets from 2014).

1 SCOPE

This standard specifies requirements for asset registration companies providing third party secure asset registration services within the UK* such that the information they are responsible for registering and maintaining:

- is secure.
- can be used to verify the identity of the registered keeper of an asset registered on the secure asset register.

The standard covers secure asset registration services based on systems that accommodate the receipt, processing and storage of information and enquiries submitted to the asset registration company by post, fax, telephone, email and internet.

The standard does not specify any one particular design of secure asset register and is applicable to all sizes of asset registration company.

The minimum security requirements defined in this standard are designed to prevent unauthorized viewing, manipulation or destruction of the information registered on secure asset registers while also ensuring that information is suitably accessible to:

- registered keepers of assets registered on the secure asset register; and
- those wishing to verify details of the registered keeper, for example, law enforcement officers or people considering purchasing the registered items.

The standard identifies four grades of secure asset register. These are defined according to the value of the equipment recorded on that secure asset register.

Note: The grades have been structured to suit the registration of individual items of the following values:

- *Grade 1 - items worth up to £20,000*
- *Grade 2 - items worth between £20,000 and £100,000*
- *Grade 3 - items worth between £100,000 and £1,000,000*
- *Grade 4 - items worth over £1,000,000*

This information shall only be used as an indication of the grading structure and shall not form the basis of any decisions on which grade of secure asset register to use to register items. Such decisions should be based on users own risk assessment together with the requirements of their insurer and guidance provided by law enforcement officers and security experts.

---

* *Although the legal framework within which this standard has been developed has resulted in its scope being restricted to companies providing secure asset registration services within UK the requirements may also be applicable to secure asset registration services provided in other countries.*

In order to achieve a grading to this standard, the asset registration company shall demonstrate compliance with all clauses relevant to the methods by which they receive, process, store and issue information securely and technologies they use.

The standard supports the secure registration of assets marked using asset marking devices approved to the following standards:

LPS 1225: Issue 3 - *Requirements for the LPCB approval and listing of asset marking systems*.

LPS 1669 (draft) - Specification for testing and classifying "microdot" asset marking devices

LPS 1650: Issue 1 - *Requirements and testing procedures for the LPCB approval and listing of 'theft resistant' electronic products*

LPS 1651 (draft) - *Requirements for the LPCB Approval and Listing of 'forensic' asset marking systems*

The standard does not preclude the use of secure asset registers to store information relating to assets that are not marked with asset marking devices certificated to the above standards.

Note: Registration of assets on secure asset registers complying with this standard does not automatically mean the registered keeper is the legal owner. Those wishing to verify legal ownership should seek additional evidence.

2 DEFINITIONS

The definitions provided in ISO 9001 *Quality management systems. Requirements* and BS EN ISO/IEC 27001: 2005 *Information technology - Security techniques - Information security management systems – Requirements apply* together with the following:

2.1 Access privilege

The scope of the secure information and/or areas within the asset registration company's facilities to which a person is authorised to have access and the degree to which they are permitted to create/edit/delete/dispose of information to which they have access.

2.2 Asset identification code

Series of at least four alphabetic and/or numeric characters incorporated on an overt marking device and is registered on a nominated secure asset register.

2.3 Asset marking device

A method of securely marking or tagging an asset to provide visible information uniquely linking that asset, via a nominated secure asset register, to the registered keeper of the asset.

2.4 Asset marking system

Coalition of marking devices (either overt or overt and covert) and a secure asset register used to provide traceability of a marked asset to its registered keeper.

2.5 Asset registration company

Company providing third party secure asset registration services.

2.6 Covert asset marking device

Method of uniquely identifying the registered keeper of an asset via a nominated secure asset register, that when applied to an asset:

i) Is secure and hidden from direct view.
ii) Cannot be read with the unaided eye, assuming normal vision and average lighting conditions.

2.7 Enquirer

Any person or organisation other than the registered owner requesting secure information held on the secure asset register.

2.8 Escrow arrangement

An escrow arrangement is one which provides the asset registration company with access to the source code should certain events occur, such as the software development company failing to maintain the software or going out of business. Escrow arrangements can either be made directly between the asset registration company and the software developer or may involve a third party commonly referred to as being an Escrow agent.

2.9 Escrow agent

A third party that holds a copy of the source code and who may release the source code to the asset registration company if the software developer is unable to meet the requirements of the Escrow arrangement.

2.10 I/O device

Portable device capable of storing data. Examples include: floppy disks, CD ROMs and memory sticks.

2.11 Operator

A person employed by the asset registration company or its subcontractors that is authorised to have access to the secure information, for example to add or change secure information or answer enquiries regarding assets recorded on the secure asset register.

2.12 Overt asset marking device

Method of uniquely identifying the registered keeper of an asset via a nominated secure asset register, that when applied to an asset:

i) Is secure.
ii) Is visible.
iii) Can be read with the unaided eye, assuming average lighting conditions.
iv) Links the asset to the registered keeper.

2.13 Registered asset

Asset that is registered on the secure asset register.

2.14 Secure area

Location in which secure information is stored or processed.

2.15 Secure asset register

A system of recording the details of a registered keeper of an asset using the unique asset identification code present on the asset marking device(s) applied to the asset.

2.16 Secure information

Any information that:

- has been submitted for placing on the secure asset register;
- is recorded on the secure asset register; or
- could result in unauthorised access to such information if compromised.

The latter may include passwords, access control codes or other information relating to the security of the secure asset register.

2.17 System administrator

A person employed by the asset registration company or its subcontractors to maintain the systems on which the secure information is stored, including any software used to process or store secure information.

2.18 User

A person using the secure asset register to either register themselves as the registered keeper of an asset, report the theft or loss of a registered asset, report the finding of a registered asset or verify the identity of the registered keeper.

2.19 User authentication

Process by which a user's or operator's identity is verified by a system before providing that person with access to secure information or secure areas to which they have defined access privileges.

2.20 Vital equipment

Equipment that is vital to continued provision of the secure asset register and the security and integrity of the secure information in accordance with the requirements contained within this standard.

3 REQUIREMENTS

3.1 General requirements

This section defines requirements that are common to all asset registration companies irrespective of the technologies they use to receive registration details and process enquiries.

The asset registration company shall:

(a) hold third party certification to ISO 9001. The scope of that certification shall cover the provision of the secure asset registration service(s) to be approved to LPS 1224 and the certification shall be issued by a certification body that is accredited to BS EN ISO/IEC 17021:2006 *Conformity assessment. Requirements for bodies providing audit and certification of management systems*

(b) be registered with the Information Commissioner's Office in accordance with the requirements of the Data Protection Act 1998 and to provide the secure asset registration services in accordance with the provisions of the Data Protection Act 1998; and

(c) ensure any third party to which they subcontract elements of the information processing and management (e.g. call centres or data storage facilities) complies with clause (b) above.

3.2 Information security management system

The asset registration company shall establish and maintain a documented information security management system that ensures:

(a) the security of the information they are responsible for; and

(b) the secure asset register's compliance with all requirements of this standard.

This system shall extend to cover any outsourced processes that may affect the security of the information for which the asset registration company is responsible.

3.2.1 Scope of information security management system

The scope of the information security management system shall cover all information registered on the secure asset register and operations relating to the management and storage of information registered on the secure asset secure asset register.

Note: It is recommended the information security management system covers all information for which the asset registration company is responsible, as defined by the Data Protection Act 1998.

3.2.2 Information security management system policy

The asset registration company shall define an information security management system policy that:

(a) includes a commitment to comply with the requirements of this standard and relevant legislation
(b) provides a framework for setting and reviewing policies relating to the operation of the asset registration service and security of the information for which the asset registration company is responsible
(c) is approved by senior management
(d) is communicated to those:
- within the organisation
- independent organisations with whom the secure information is shared
- registering assets on the secure asset register
- using the secure asset register, for example, to confirm whether an asset is registered as lost or stolen, verify the identity of the registered keeper of an asset or to record a lost or stolen asset as being found

(e) is reviewed to ensure continued conformity with the requirements of this standard. These reviews shall be conducted on a periodic basis and when significant changes to the asset registration company occur.

3.2.3 Risk assessment

3.2.3.1 Although this standard outlines a series of minimum requirements in relation to the security of secure asset registers, asset registration companies are responsible for ensuring that the measures they implement are appropriate to the risks they face. The asset registration company shall therefore:

(a) identify an appropriate risk assessment methodology
(b) develop criteria for reviewing and identifying:
acceptable levels of risk
measures to control risk
(c) identify and evaluate risks, including legal and regulatory requirements

(d) identify and evaluate options for controlling risk
(e) define the risk management policy and appropriate procedures for treating the risks identified and the reason for their selection.

Note: A number of risk assessment methodologies are discussed in ISO/IEC TR 13335-3 Information technology - Guidelines for the management of IT security - Techniques for the management of security

3.2.3.2 The risk assessment shall identify the risks to the security of the information held by the asset registration company posed by anyone that may have access to the secure asset register or environment within which that secure asset register is operated. This shall consider:
(a) The facilities and secure information to which that person needs to have access.
(b) The likely frequency and duration of that access.
(c) The type of access they require, including:
- Physical access to offices, servers, secure documents
- Electronic access to the secure asset register.

(d) The type of information to which they may have access and whether that information is either covered by the Data Protection Act 1998 or could lead to a reduction in security afforded to the secure information.
(e) How the identity of those with authorised access can be verified and their activities monitored to ensure they do not compromise the secure information in any way.

3.2.4 Implementation, monitoring and review of the information security management system

The asset registration company shall:
(a) ensure the secure asset register meets all the requirements of this standard appropriate to the technologies they use to receive and process information and enquiries, as defined in clause 3.4
(b) communicate the information security management system policy and procedures to all staff and subcontractors that have access to the information, facilities and equipment falling with the scope of the information security management system
(c) implement the procedures defined within the information security management system
(d) manage the operation of the information security management system and resources required to operate the information security management system
(e) define and implement measures for monitoring and reviewing the effectiveness of the information security management system
(f) implement procedures for detecting and responding to security events and incidents.

3.2.5 Information security management system documentation

The asset registration company shall establish and maintain documentation supporting the management of the secure asset register in accordance with this standard and ISO 9001.

The documentation shall include the following:

(a) The scope of the information security management system (see clause 3.2.1).
(b) The information security management system policy statement (see clause 3.2.2).
(c) Risk assessment methods used to establish the information security management system procedures and controls (see clause 3.2.3(a)) and records of the risk assessments undertaken.
(d) Procedures and controls that support the information security management system policy.
(e) Documents defining the information required when users wish to:
    - register assets
    - change their details or those of assets they have registered on the secure asset register
    - search for assets
    - record the loss, theft or recovery of registered assets
    - remove assets from the register.
(f) Records produced using information supplied by those using the asset register or to demonstrate the asset registration company's conformity with the requirements of this standard. These shall include:
    i) Information recorded on the secure asset register and records of changes to information recorded on the secure asset register.
    ii) Records of enquiries made in relation to items registered on the secure asset register and records of the information provided.
    iii) Records of security incidents.
    iv) Records of personnel having access to information recorded on the secure asset register or to information that may provide.

The documentation may be in a physical format or electronic format.

3.2.6 Document control

3.2.6.1 Documents required by the information security management system shall be controlled in accordance with a defined set of procedures that comply with the requirements of clause 4.2.3 of ISO 9001.

3.2.6.2 Access privileges relating to each document shall be defined. The privileges shall define who may have access to the document and what editorial rights they have in relation to that document. The access privileges shall take into account the security of the information contained on the document and the need for people to have access to the information contained on that document.

3.2.7 Record maintenance

3.2.7.1 Records shall be maintained in accordance with procedures that comply with the requirements of clause 4.2.4 of ISO 9001.

3.2.8 Management responsibility

3.2.8.1 Management shall provide evidence of their commitment to the establishment and implementation of an effective information security management system in accordance with the requirements of this standard by:

(a) establishing the information security management system policy, objectives and controls;
(b) defining the criteria for evaluating risk; and
(c) communicating the importance of complying with the requirements of this standard and legal obligations and the need to continually improve.

3.2.8.2 Management shall define roles and responsibilities for information security and shall provide sufficient resource to establish and maintain the secure asset registration service in accordance with the requirements of this standard and ISO 9001.

3.2.8.3 Management shall ensure regular internal audits are conducted in accordance with the requirements of clause 3.2.12 and that appropriate actions are taken to resolve any issues highlighted during those audits.

3.2.8.4 Management shall conduct reviews of the information security management system at least once a year to ensure their continued suitability, adequacy and effectiveness and identify opportunities for improvement. These shall be conducted in accordance with the requirements of clause 5.6 of ISO 9001 and shall cover the inputs specified in clause 5.6.2 of ISO 9001 together with the following:

- Results of audits of the information security management system.
- Results of previous risk assessments in light of current knowledge and best practice to confirm whether remain suitable and to ensure all known risks are covered.

3.2.9 Resource management

3.2.9.1 There shall be sufficient resource to:

(a) operate the secure asset register in accordance with the requirements of this standard; and
(b) maintain the service levels stated in accordance with clause 3.2.16.

3.2.9.2 Secure asset register loading shall be monitored to ensure timely action is taken to increase capacity when required. Capacity requirements shall be monitored to indicate where action is needed to avoid failures due to inadequate resources.

3.2.9.3 Equipment on which continued operation of the secure asset register relies shall be maintained in accordance with the manufacturer's recommendations and periodic checks conducted to ensure equipment is replaced before its condition deteriorates

beyond a point at which the data stored on or processed by that equipment could be compromised as a result of that deterioration.

3.2.9.4 The clocks on all information processing systems associated with the storage and retrieval of information on the secure asset register shall be synchronised with a common accurate time source and this shall be periodically checked. The time source against which the clocks are synchronised shall be defined.

3.2.9.5 The following shall be logged in order to detect unauthorised information processing activities:

- User activities and exceptions.
- System administrator and operator activities.
- Faults.

3.2.9.6 The logs shall be regularly analysed and appropriate action taken.

3.2.10 Event logs

3.2.10.1 The following operations and events shall be logged to support detection of potential breaches in information security and investigations should any security breaches occur:

(a) Issue of, and changes to, user IDs and passwords.
(b) Unsuccessful access attempts, either to the secure asset register or through building access control systems controlling access to the secure areas.
(c) Activation, deactivation or changes to the protection system settings, such as those relating to anti-virus systems, access control devices and alarm systems.
(d) The use of privileges to start-up or stop the system, access account information or attach/detach I/O devices.

In addition, the identities, dates and times of people logging on and off the secure asset register shall be logged on grade 3 and 4 registers.

3.2.10.2 The event logs shall include system administrator's activities and system administrators shall not have the necessary permissions to amend or deactivate logs of their own activities.

3.2.10.3 Event logs shall be write protected and shall be stored in a secure area.

3.2.10.4 Events shall be reviewed to detect unauthorised and unusual activity.

Note: Audit software may be used to check for unauthorised and unusual activity.

3.2.11 Incident response

3.2.11.1 The asset registration company shall establish and maintain a system for identifying, reporting, investigating and responding to the following:

- Unauthorised activity.
- Security incidents.
- Faults.

Notes: *(1) Faults that are to be covered include data errors, software malfunctions, power failures, website going off-line.*

(2) Asset registration companies should consider the guidance on information security incident management provided in PD ISO/IEC TR 18044: 2004 Information technology - Security techniques - Information security incident management.

3.2.11.2 All staff, contractors and users shall be advised of the need to report security incidents, faults and errors.

3.2.11.3 Procedures for dealing with unauthorised and unusual activity shall ensure:

(a) Unauthorised and unusual activity is investigated to identify whether security has been breached and, if so, what effect they have had on the information contained on the secure asset register.
(b) Appropriate corrective action is implemented in a timely fashion to ensure the information held on the secure asset register is complete and accurate.
(c) Appropriate preventative action is implemented in a timely fashion to ensure future security breaches of the types identified cannot occur.

3.2.11.4 All security incidents shall be recorded and those records shall include the following:

(a) The nature of the incident/fault.
(b) Details of who reported the incident and, if different, who recorded the incident.
(c) When the incident occurred and was reported.
(d) The nature of any investigations conducted into the cause of the incident and their likely impact on the integrity of the secure information, and the results of those investigations.
(e) The nature of any corrective and preventative actions implemented as a result of that incident.

Note: *If the incident is likely to result in legal proceedings then the evidence shall be collated and maintained in accordance with local judicial guidance.*

3.2.11.5 If the incident involves detection of a virus, the actions taken shall include the following:

(a) Isolating all infected systems, disks and other storage media.
(b) All traces of virus shall be removed.
(c) Media exchange systems shall be suspended until both the systems and media are clean.

3.2.11.6 Incident records shall be maintained in accordance with clause 3.2.7.

3.2.11.7 Faults reported by users, operators or systems software shall be logged.

3.2.11.8 Procedures for dealing with faults shall ensure:
(a) Appropriate corrective actions are implemented to resolve each fault and any subsequent effect those faults may have had on the accuracy of the information held on the secure asset register.
(b) Appropriate preventative actions are implemented to prevent the fault reoccurring.

3.2.11.9 Fault logs shall be reviewed on a regular basis to ensure all are addressed in good time and that any trends are identified and investigated and appropriate corrective and preventative action implemented. The frequency of these reviews shall be set according to the nature and frequency of faults occurring and their possible effects on the accuracy of the information held on the secure asset register.

3.2.11.10 Management shall be responsible for ensuring all reported incidents are dealt with quickly and effectively.

3.2.12 Internal audits

3.2.12.1 The asset registration company shall define and implement procedures for conducting internal audits, recording the results of audits and maintaining records of the audits.

The purpose of the audits shall be to determine whether the asset registration company continues to conform to the requirements identified within:
(a) this standard.
(b) ISO 9001
(c) the information security management system and quality systems; and
(d) relevant legislation.

3.2.12.2 Internal audits shall be conducted at planned intervals that take into account:
(a) the status and importance of the processes and areas being audited
(b) the results of previous audits
(c) changes to the company, the manner in which it handles information, its information security management or quality systems; and
(d) any incidents that have occurred.

3.2.12.3 The selection of auditors shall ensure objectivity and impartiality of the audit process.

3.2.12.4 Independent penetration tests of the system shall be conducted on grade 3 and 4 secure asset registers before the secure asset register is launched and then:
(a) at least once every three years
(b) when there is a major change to the system or software; or
(c) the secure information is compromised by a security incident.

3.2.12.5 The penetration tests shall be conducted by qualified penetration testers. Examples include those operating within the following schemes:

- CHECK†
- CREST‡

3.2.12.6 The asset registration company shall implement timely corrective and preventative actions that comply with the requirements of clause 3.2.13 and that address:

(a) non-conformities identified during the audits
(b) risks identified during the audits for which current security measures are not considered appropriate.

3.2.12.7 Records of internal audits and penetration tests shall be maintained in accordance with clause 3.2.7.

3.2.13 Corrective and preventative actions

3.2.13.1 The asset registration company shall define and implement document procedures for implementing corrective actions to eliminate the cause of existing or previous non-conformities. The procedures shall define how to:

(a) Identify non-conformities and determine their cause.
(b) Review the need to implement corrective actions, determine appropriate actions and implement those actions.
(c) Record the results of the review of the non-conformity and the corrective actions taken.
(d) Review the effectiveness of the corrective actions taken and record the results of that review.

3.2.13.2 The asset registration company shall define and implement document procedures for implementing preventative actions to eliminate the cause of potential non-conformities. The procedures shall define how to:

(a) Identify potential non-conformities, determine their cause and identify their likely impact on the asset registration company's compliance with the requirements of this standard.
(b) Review the need to implement preventative actions, determine appropriate actions and implement those actions.
(c) Record the results of the review of the potential non-conformity and the preventative actions taken.
(d) Review the effectiveness of the preventative actions taken and record the results of that review.

3.2.13.3 Records of corrective and preventative action shall be maintained in accordance with clause 3.2.7.

---

† *The Communications and Electronic Security Group (CESG) operates this scheme. Details of the scheme and a list of licensed CHECK testers can be obtained from www.cesg.gov.uk.*

‡ *This Council of Registered Ethical Security Testers operates this scheme. Details of the scheme and a list of licensed CREST testers can be obtained from www.crest-approved.org.*

3.2.14 Maintenance

3.2.14.1 Regular and frequent back-ups of all secure information shall be made, and these shall be 128 bit encrypted to prevent unauthorised use.

3.2.14.2 Backup copies should be stored away from the location from which the information has been backed-up. The back-up information shall be afforded similar physical and environmental security as that applied to the information being backed up.

3.2.14.3 Records of all back-ups shall be maintained.

3.2.14.4 The frequency of the back-ups should be determined according to the volume of information processed by the system and the ability to update the secure asset register using those backups should a failure of the secure asset register occur.

3.2.14.5 The back-ups shall be regularly tested to ensure their suitability for restoring the secure asset register and a record of those tests maintained.

3.2.14.6 Restoration procedures shall be defined and regularly checked to ensure the secure asset register can be restored in accordance with clause 3.2.15.

3.2.14.7 Secure asset register loading shall be monitored to ensure timely action is taken to increase capacity when required. Capacity requirements shall be monitored to indicate where action is needed to avoid failures due to inadequate resources.

3.2.14.8 Criteria for accepting IT system changes and upgrades shall be established and documented.

3.2.14.9 Appropriate tests and/or reviews of the changes/upgrades shall be conducted off-line and approved prior to implementation. These tests shall not use live data.

3.2.15 Business continuity

3.2.15.1 A business continuity procedure shall be implemented and shall ensure:

(a) the asset registration company can operate the secure asset register within 24 hours of a major event/incident that affects the provision of the secure asset registration service occurring.

(b) minor events/incidents do not undermine the asset registration company's conformity with the service level they define in accordance with clause 3.2.16.1.

3.2.15.2 The continuity plan shall be tested and reviewed on a regular basis, and updated accordingly to ensure its continued effectiveness.

3.2.15.3 The continuity plan shall ensure compliance with the requirements of this standard is maintained, with the exception of clause 3.2.16 for the period defined in clause 3.2.15.1.

Note: It is particularly important to consider the possible effects of any resultant changes to the locations used to operate the secure asset register or people having operator or administrative access to the information being registered and stored on the secure asset register.

Further guidance on continuity planning is provided in standard BS 25999-1:2006 Business continuity management. Part 1: Code of practice.

3.2.15.4 In the event of the asset registration company ceasing trading, changing ownership or contact details, such as postal/e-mail address or telephone number, the asset registration company shall inform all parties affected by the change, including LPCB.

3.2.15.5 If the asset registration company is to cease trading it shall first provide written confirmation of the provisions made for future storage and access of the information held on the secure asset register to all registered users and LPCB.

Note: The asset registration company should have in place an escrow arrangement with, where possible, another asset registration company approved to LPS 1224. The escrow arrangement should permit the other asset registration company to take over the operation of the secure asset register and have access to the source code in the event that the asset registration company is unable to continue to run the secure asset register in accordance with LPS 1224. Such arrangements should be communicated to users in accordance with the provisions of the Data Protection Act 1998.

3.2.16 Service level

3.2.16.1 The asset registration company shall publish their service level in terms of:

(a) The methods by which they can receive enquiries, for example telephone, facsimile, letter, email and internet.
(b) Their average timescales for processing information submitted by each of those methods and for responding to enquiries.
(c) The period used to determine that service level.

Notes: (i) The asset registration company should advertise the above in website, sales literature or other documents and should form part of the contract that users agree to when signing up to use the secure asset register.

(ii) Due consideration should be given to the Trade Descriptions Act when making statements regarding service level and to ensuring the service level identified can be achieved even in unexpected

situations, such as those requiring implementation of the continuity procedures required in clause 3.2.15.

(iii) The timescales for responding to enquiries may differ according to the methods by which the enquiries are submitted to the asset registration company, the quality of the information submitted and the type of asset marking technology used to identify the asset. For example, it may take longer to confirm the identity of registered keepers of assets marked using forensic chemicals than products marked with overt asset marking systems approved to LPS 1225.

3.2.16.2 The timescales for responding to enquiries shall be based on the results of regular reviews conducted in accordance with clause 3.2.16.4. They shall be defined in terms of the average response time achieved by the company.

3.2.16.3 The period used to calculate service level shall be at least 3 months but no longer than one year.

3.2.16.4 The asset registration companies shall record all enquiries received and actions taken to resolve those enquiries. These records shall indicate the time taken to answer each enquiry received.

3.2.16.5 The asset registration company shall publish all fees payable by members of the public and law enforcement officers in relation to the following activities:

- registration of assets and/or users
- changing details
- reporting assets as lost or stolen
- checking information held on the database
- cancelling user/asset registration

3.3 Resources

3.3.1 Information processing facilities

3.3.1.1 The security of all facilities used to store or process secure information shall meet the requirements of clause 3.3.2.

3.3.1.2 All personnel at facilities used to store or process secure information shall be checked to ensure they meet the requirements of clause 3.3.3 and regular reviews conducted to ensure continued compliance.

3.3.1.3 All hardware and software shall be checked to ensure they are compatible with other system components before being implemented.

3.3.1.4 All reviews shall be conducted and approved by competent persons and records of those reviews maintained in accordance with clause 3.2.7.

3.3.2 Physical security and other protection of facilities

3.3.2.1 Operations relating to the processing and storage of information on the secure asset register; such as information entry, processing, storage and destruction; shall be located in secure areas within a protected building.

3.3.2.2 No means of directly identifying the information processing activities conducted within the building shall be present on or around buildings used for operations relating to the processing and storage of information on secure asset register of grades 2 and above.

3.3.2.3 The secure areas shall have defined security perimeters and strategically located barriers with, where appropriate, electronic surveillance and/or alarming systems in place. It is recommended these meet the requirements defined in Table 1.

Note: It is recommended that other aspects of the secure area's perimeter are reviewed and, where necessary, upgraded to ensure they provide resistance to penetration consistent with the minimum security performance of the doors to that secure area.

The asset registration company must ensure the ability of occupants to escape in an emergency when specifying the design and functionality of doors, windows and other security barriers.

Table 1 Recommended minimum performance of doors, windows and alarm systems used to protect secure areas.

Grade	**Minimum security**			
	Doors	**Windows and/or supplementary protection**	**Alarm system**	**CCTV**
1	Lockable doors with access keys/tokens/ codes only issued to those with appropriate access privileges. *Note: It is recommended that these meet PAS24-1.*	Lockable windows. *Note: It is recommended that these meet BS 7950.*	Bells only[(i)]	-
2	PAS 24-1 or SR1 to LPS 1175.	BS 7950 or SR1 to LPS 1175.	Monitored[(ii)(iii)] *Note: It is recommended that the system meets the requirements of Grade 2 defined in EN 50131-1: 2006.*	Y[(iv)]
3	SR2 to LPS 1175	SR2 to LPS 1175	Monitored[(ii)(iii)] *Note: It is recommended that the system meets the requirements of Grade 3 defined in EN 50131-1: 2006.*	Y[(iv)]
4	SR3 to LPS 1175	SR3 to LPS 1175	Monitored[(ii)(iii)] *Note: It is recommended that the system meets the requirements of Grade 4 defined in EN 50131-1: 2006.*	Y[(iv)]

Notes:

(i) If the secure area is not manned 24 hours every day, the alarm system should be monitored[(ii)] and should meet the requirements of Grade 2 defined in EN 50131-1: 2006 and the alarm notification meet requirements of option C in clause 8.6 of EN 50131-1: 2006.

(ii) Alarm installation and monitoring should be in accordance with the requirements contained in the Association of Chief Police Officers' (ACPO) publication 'Police Response to Security Systems' dated November 2006.

(iii) Monitored personal attack alarms should be made available to those working in the secure area.

(iv) The CCTV system shall, at minimum, record movement of people between secure areas and adjacent areas, and should meet the requirements of BS 8418: 2003 *Installation and remote monitoring of detector activated CCTV systems. Code of practice.*

3.3.2.4 Entry to the secure area shall be controlled such that only authorised personnel have access to that area. An auditable record of access to the secure area shall be maintained for areas relating to the processing and storage of information on secure asset register of grades 3 and 4.

Note: It is important to ensure the layout of the building is carefully considered to ensure occupants are able to exit the building safely in an emergency and that this does not require them to pass through restricted areas to which they do not have defined access privileges.

3.3.2.5 All people within the secure area shall wear visible identification.

Note: In smaller companies where the staff all know one another it may be possible, as an alternative to all staff wearing visible identification, for the asset registration company to:
(i) Require all visitors to wear identification; and/or
(ii) Demonstrate that all members of their staff authorised to work in the secure area will immediately raise the alarm if an unauthorised person is unaccompanied at any time within the secure area.

3.3.2.6 Anyone that is not authorised to have access to the secured information stored or processed in a secure area shall be accompanied at all times when in the secured area and appropriate measures shall be enforced to ensure they do not have access to any such secured information.

3.3.2.7 Other areas within the building that hold supporting functions involving sensitive information shall be afforded the same level of protection as that provided to the secure asset register. Examples include areas used for the storage of personnel records and passwords.

3.3.2.8 Procedures for controlling the use of doors between secure and non-secure areas shall be implemented to prevent unauthorised access, for example, by tailgating.

3.3.2.9 Access privileges to secure areas shall be regularly reviewed and updated as necessary. Records of those reviews shall be maintained in accordance with clause 3.2.7.

3.3.2.10 The building's vulnerabilities to natural and environmental hazards should be considered and appropriate measures implemented to mitigate those hazards. Examples include fire, flood and explosion.

3.3.2.11 Workstations and other equipment with visible screens and any paper records containing secure information shall be orientated and/or stored in such a way as to prevent unauthorised viewing e.g. from public areas or by people that may have access to the secure room but who are not authorised to view the secure information.

3.3.2.12 All vital equipment shall be located in an environment conducive to that required within the user instructions provided with that equipment. This includes appropriate

minimum spacing around any ventilation slots and the use of devices to control the atmospheric conditions within which the equipment operates.

3.3.2.13 An uninterruptable power supply (UPS) shall be fitted to vital equipment and power continuity plans implemented in accordance with clause 3.2.15 to cover failure of the UPS.

3.3.2.14 Telecommunications equipment used on grade 3 and 4 secure asset registers shall be linked to the utility provider by at least two different routes.

3.3.3 Personnel

3.3.3.1 Only authorised personnel shall have access to information held on the secure asset register.

3.3.3.2 All personnel or third party organisations assigned responsibilities within the information security management system shall be competent to perform the task. The asset registration company shall therefore define:

- The minimum competency required to fulfil the various roles in support of the provision of the secure asset registration service.
- The method by which competency will be checked and any actions that will be taken to resolve shortfalls in the competency.
- The competency records to be maintained.

3.3.3.3 All personnel or third party organisations assigned responsibilities within the information security management system shall be aware of the relevance and importance of the information security activities and how they contribute to the asset registration company's compliance with the requirements of this standard and all relevant legal obligations.

3.3.3.4 Prior to being given access to the secure asset register, all new personnel shall:

i) Successfully undergo security vetting in accordance with BS 7858: 2006 *Security screening of individuals employed in a security environment - Code of practice.* Existing personnel that have an exemplary security record with the company and have been in regular employment with the asset registration company since before this standard was published or for a period of at least one year, whichever is the longer, are deemed to meet the requirements of this standard without the need for further security vetting.

Note: All company's have a statutory duty to ensure all their staff have the 'right to work' within the country in which they are to be employed and the company should retain appropriate evidence of the checks carried out and the results of those checks.

ii) Sign a confidentiality agreement complying with clause 3.3.4.
iii) Be assigned an individual password, as defined in clause 3.4.8.1.

3.3.3.5 Records of the employee vetting, confidentiality agreement and password issue shall be maintained in accordance with clause 3.2.7 in a secure environment accessible only by authorised personnel.

3.3.3.6 All employees and contractors shall be advised of the formal disciplinary procedures and security breaches by employees or contractors dealt with through the formal disciplinary procedure. Records of all disciplinary action shall be maintained.

3.3.3.7 Employees and contractors shall agree and sign terms and conditions of employment or contract and the terms shall define the employee/contractor's and asset registration company's responsibilities in respect to information security, as defined within clause 3.3.4.

3.3.3.8 The security roles and responsibilities of each of the asset registration company's employees and contractors shall be defined. These should include any general responsibilities for implementing or maintaining security policy, together with specific responsibilities, for example the protection of particular assets or the execution of particular security processes.

3.3.3.9 Staff and contractors shall be issued with the following:

(a) Photographic identification confirming their identification and access privileges, where required in clause 3.3.2.5.
(b) Keys/access codes/tokens enabling them to access to those areas and into those containers to which they have defined access privileges.

Note: It is recommended that either electronic access control devices are used to control access to rooms/containers and that; if locks requiring mechanical keys are used; the issue of keys to staff and contractors is managed using an auditable key management system.

3.3.3.10 The access privileges of employees and contractors shall be immediately removed during any period of suspension from work or upon termination of their employment, contract or agreement, or suitably adjusted to reflect any changes to their role within the organisation.

3.3.4 Confidentiality agreement

3.3.4.1 All employees and contractors that are likely to have access to the secure information shall sign confidentiality agreements. These shall define:

(a) The information to be protected.
(b) Expected duration of the agreement including cases that may require the secure information to be divulged to others (e.g. when a warrant is received requiring the release of particular information/records) or may need to be maintained indefinitely.

Note: It is important to consider the requirements of the Data Protection Act 1998 when drawing up this aspect of the confidentiality agreement.

(c) Responsibilities and actions of signatories when the agreement is terminated.
(d) Responsibilities and actions of signatories to avoid unauthorised disclosure.
(e) Responsibilities and required actions of signatories in the event of unauthorised disclosure of the secure information and/or a breach of the agreement.

Note: This may form part of the contract of employment and of terms and conditions of purchasing products and services.

3.3.4.2 Copies of all signed confidentiality agreements shall be maintained in accordance with clause 3.2.7.

3.3.5 Outsourced services

3.3.5.1 Outsourced services shall be managed in accordance with the requirements of this standard and ISO 9001.

3.3.5.2 Suppliers of outsourced services shall be vetted to ensure they are appropriately qualified and can provide that service in accordance with the relevant clauses of this standard. Records of any checks undertaken shall be maintained in accordance with clause 3.2.7.

3.3.5.3 All outsourced services shall be covered by a contract and compliance with the terms of the contract shall be monitored and regularly reviewed. Copies of those contracts shall be maintained in accordance with clause 3.2.7.

3.3.5.4 The asset registration company is responsible for ensuring that any secure information to which that supplier has access is afforded equivalent security to that provided by the asset registration company and that their suppliers comply with the relevant clauses of this standard.

3.3.5.5 Outsourced software development shall be supported by:
(a) Quality system certification
(b) Contracts covering:
- rights of access for audit of the quality and accuracy of the work and security of the work undertaken for the asset registration company
- requirements for quality, functionality and security of the code, including detection of malicious code
- intellectual property rights; and
- escrow arrangements to protect the asset registration company in the event of failure of the software development company.

Copies of these records shall be maintained in accordance with clause 3.2.7.

3.3.6 Protection of electronic information

3.3.6.1 Access to secure information held electronically shall be restricted to those with appropriate access privileges, in accordance with clause 3.4.7.6.

3.3.6.2 Access to source code shall be restricted such that only those with the appropriate access privileges defined within the information security management system can view and edit the source code.

3.3.6.3 The use of unauthorised software shall be prohibited.

3.3.6.4 The use of auto-forwarding facilities on email based accounts designed to receive and process secure information and enquiries shall be prohibited unless restricted to forwarding information to others with defined access privileges covering that information being forwarded.

3.3.6.5 Software and information content relating to systems supporting registration, storage and processing of secure information shall be regularly checked to ensure any unauthorised files or amendments are investigated.

3.3.6.6 Measures to protect the secure information against malicious code shall:
(a) include prevention, detection and recovery measures
(b) be planned and implemented and their effectiveness regularly reviewed.

3.3.6.7 Malicious code detection and repair software shall be installed and kept up to date. The software shall automatically check for the following:
(a) Files received via networks or on electronic or optical media.
(b) Electronic mail attachments and downloads.
(c) Code attached to web pages.

3.3.6.8 A time-out facility shall clear the screen on a terminal if there is no activity on that terminal for any duration longer than that defined in Table 2. This shall require the user to enter a password complying with 3.4.8.

Table 2 Maximum period before time-out facility clears the screen when there is no activity on that database terminal

Grade	Maximum Time *(Minutes)*
1	10
2	7
3	5
4	3

Note: This may be achieved via a password activated screensaver or other automatically triggered information access protection device.

3.3.6.9 A person's access to the secure asset register shall be shut down after the periods of inactivity specified in Table 3 and shall require them to re-enter their user ID and password before regaining access to the secure asset register.

Table 3 Maximum period of inactivity prior to automatic shut down of access to the database

Grade	Maximum period of inactivity *(Minutes)*
1	20
2	15
3	10
4	5

3.3.6.10 A session time-out facility shall prevent users from being logged onto the secure asset register for longer than the maximum session times specified in Table 4 and shall require them to re-enter their user ID and password before regaining access to the secure asset register.

Table 4 Maximum session duration

Grade	Maximum user session durations *(Minutes)*	
	Page	Total session
1	10	15
2	7	15
3	5	15
4	3	15

Note: This requirement also applies to operators accessing the system over an internet or wireless connection.

3.4 Access to secure information

3.4.1 Information exchange policy

3.4.1.1 The asset registration company shall implement a policy for exchange of secure information. This should cover those third parties:

i) registering assets on the secure asset register
ii) searching for assets on the secure asset register
iii) reporting assets as lost or stolen
iv) reporting assets as found
v) transferring ownership or otherwise updating ownership information.

3.4.1.2 The information exchange policy shall cover secure information transferred electronically (e.g. via email and internet), physically (e.g. by post or in person), by telephone and by fax.

3.4.1.3 The information exchange policy shall:

i) Require the authentication of the person with whom the secure information is being exchanged.
ii) Define the secure information that can be exchanged. This shall be restricted to that information covered by their defined access rights. Those

rights shall themselves be restricted to only including the following information:

- A general user's access shall be restricted to the following:
  - creating and updating their account
  - registering assets on the secure asset register
  - searching for assets on the secure asset register
  - reporting assets as lost or stolen
  - reporting assets as found
- A registered keeper's access shall be restricted to that:
  - which a general user is restricted to;
  - reviewing and updating details of assets registered to them
- A service provider's access shall be restricted to that they need in order for them to provide the service required by the asset registration company.

iii) Ensure appropriate protection of the exchanged information to prevent unauthorised interception, copying or modification.

iv) Require the recording of exchanges of secure information and review of those records to identify unusual or non-conformant transactions.

3.4.1.4 The information exchange policy shall ensure secure information relating to assets or registered keepers is only shared with nominated third parties and then only when all of the following are true:

i) The third party's access privileges include access to that information.

ii) The registered keeper has given their permission for that information to be shared with that third party.

3.4.1.5 Before permitting a third party to undertake any of the activities listed in clause 3.4.1.1, or giving them access to secure areas, the asset registration company shall advise that third party of the asset registration company's information security policy and require them to sign up to terms of use and confidentiality agreement (clause 3.3.4). The terms of use shall cover the following:

(a) Description of the service(s) to be provided and target service level (clause 3.2.16).

(b) Restrictions on copying or disclosing secure information.

(c) Access control policy including permitted access methods, the control and use of user ID and passwords, authentication process for users and termination of access privileges.

(d) Arrangements for reporting and investigating information inaccuracies, information security incidents and breaches in security, confidentiality requirements or other contract terms.

(e) The right to monitor usage and revoke access.

(f) Liabilities of the user and asset registration company.

3.4.1.6 Access to secure information shall be managed in accordance with clause 3.4.7.

3.4.2 Exchange of secure information by telephone

3.4.2.1 The asset registration company shall ensure that the advertised telephone number(s) for the secure asset register cannot be rerouted to a third party that does not have authorised administrator access to the secure asset register.

3.4.2.2 Users shall be advised if the telephone calls are recorded or monitored, for example, for security or training purposes.

3.4.2.3 The use of answering machines or voice mail to log messages must be monitored to ensure only authorised personnel can review messages left on the answering machine.

Note: This may be achieved through use of password control facilities on answering machines/voice mail systems.

3.4.2.4 The asset registration company shall not provide registered keeper's details over the telephone.

3.4.2.5 The asset registration company may provide a 'yes'/'no' answer to the question "Is asset '####' registered as lost or stolen?" (where #### is the asset registration number marked on the asset) to a general enquirer.

3.4.2.6 The asset registration company may provide a 'yes'/'no' answer to the question "Is 'x' the registered keeper of asset '####'?" (where #### is the asset registration number marked on the asset) to an enquirer. This is providing:

(a) the enquirer has appropriate access privileges, and
(b) the telephone number dialled in order to contact the enquirer is the registered contact telephone number for that enquirer, and
(c) a system of checking the telephone number is implemented to ensure the correct number is dialled.

3.4.2.7 The asset registration company shall not provide anyone other than the registered keeper or law enforcement officer's access to any secure information about the assets or keepers stored on grade 2, 3 or 4 secure asset registers other than that information covered in clauses 3.4.2.5 and 3.4.2.6.

3.4.2.8 The asset registration company may provide access to information about the assets or confirm the keeper's details stored on grade 1 secure asset registers to enquirer's other than the associated registered keeper or law enforcement officers if:

(a) the enquirer's ID has been authenticated, and
(b) the enquirer has appropriate access privileges, including permission from the registered keeper that the information may be supplied to that enquirer, and
(c) the telephone number dialled in order to contact the enquirer is the registered contact telephone number for that enquirer, and
(d) a system of checking the telephone number is implemented to ensure the correct number is dialled.

3.4.3 Exchange of secure information via the internet

3.4.3.1 If access to the secure asset register is to be provided over a network linked to the internet either directly or via common equipment (e.g. servers):

(a) That network shall take the form of a secure connection complying with Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocols for which access requires validation involving entry of a correct combination of user ID and password(s).

(b) The information shall be commercially encrypted such that only authorised parties may access the information.

(c) Firewalls and anti-virus software shall be installed and operated to protect the secure asset register and shall be kept up to date. These shall either include or be supported by up to date intrusion detection systems.

Note: Asset registration companies should consider using intruder detection systems that comply with ISO/IEC 18043: 2006 Information technology. Security techniques. Selection, deployment and operations of intrusion detection systems.

3.4.3.2 On-line transactions shall be protected to prevent incomplete transmission, miss-routing, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay.

3.4.3.3 The secure asset register may provide a 'yes'/'no' answer to the question "Is asset '####' registered as lost or stolen?" (where #### is the asset registration number marked on the asset) to a general enquirer that is registered to use the secure asset register.

3.4.3.4 The asset registration company may provide a 'yes'/'no' answer to the question "Is 'x' the registered keeper of asset '####'?" (where #### is the asset registration number marked on the asset) to an enquirer providing:

(a) the enquirer has appropriate access privileges, and

(b) the enquirer is logged into the secure asset register in accordance with clause 3.4.3.1.

3.4.3.5 The asset registration company may provide access to additional information about the asset and registered keeper to law enforcement officers if:

(a) the access to the register is via a secure server link with the Police National Computer (PNC), and

(b) the registered keeper has agreed to the information being supplied to law enforcement officers or the asset registration company is otherwise required by law to release that information.

3.4.3.6 The asset registration company shall not provide anyone other than the registered keeper or law enforcement officer's access to any secure information about the assets or keepers stored on grade 2, 3 or 4 secure asset registers other than that information covered in clauses 3.4.3.4 and 3.4.3.5.

3.4.3.7 The asset registration company may provide access to information about the assets or confirm the keeper's details stored on grade 1 secure asset registers to enquirer's other than the associated registered keeper or law enforcement officers if:

(a) the enquirer has appropriate access privileges, including permission from the registered keeper that the information may be supplied to that enquirer, and
(b) the enquirer is logged into the secure asset register in accordance with clause 3.4.3.1.

3.4.4 Exchange of secure information by email

3.4.4.1 The secure asset register may provide a 'yes'/'no' answer to the question "Is asset '####' registered as lost or stolen?" (where #### is the asset registration number marked on the asset) to a general enquirer that is registered to use the secure asset register.

3.4.4.2 The asset registration company may provide a 'yes'/'no' answer to the question "Is 'x' the registered keeper of asset '####'?" (where #### is the asset registration number marked on the asset) to an enquirer providing:

(a) the enquirer has appropriate access privileges, and
(b) the email is sent to that enquirers registered email address.

3.4.4.3 The asset registration company may provide access to additional information about the asset and registered keeper to law enforcement officers if:

(a) the asset to which the details relate is registered as lost or stolen
(b) the information is supplied via their registered Police National Network (PNN) email account, and
(c) the registered keeper has agreed to the information being supplied to law enforcement officers or the asset registration company is otherwise required by law to release that information.

3.4.4.4 The asset registration company shall not provide anyone other than the registered keeper or law enforcement officer's access to any secure information about the assets or keepers stored on grade 2, 3 or 4 secure asset registers other than that information covered in clauses 3.4.4.2 and 3.4.4.3.

3.4.4.5 The asset registration company may provide access to information about the assets or confirm the keeper's details stored on grade 1 secure asset registers to enquirer's other than the associated registered keeper or law enforcement officers if:

(a) the enquirer has appropriate access privileges, including permission from the registered keeper that the information may be supplied to that enquirer, and
(b) the email is sent to the enquirers registered email address.

3.4.4.6 Email systems shall incorporate safeguards to ensure secure information is only transmitted to registered email accounts and that it is only sent to privately accessed accounts.

Note: Secure information should not be sent to 'open' email accounts such as: 'info@company.co.uk' and 'enquiries@company.co.uk'.

3.4.4.7 All secure information contained within emails shall be encrypted. The encryption keys shall not be supplied to the recipient by email.

3.4.5 Exchange of secure information by post

3.4.5.1 The secure asset register may provide a 'yes'/'no' answer to the question "Is asset '####' registered as lost or stolen?" (where #### is the asset registration number marked on the asset) to a general enquirer that is registered to use the secure asset register.

3.4.5.2 The asset registration company may provide a 'yes'/'no' answer to the question "Is 'x' the registered keeper of asset '####'?" (where #### is the asset registration number marked on the asset) to an enquirer providing:

(a) the enquirer has appropriate access privileges, and
(b) the letter is sent to that enquirers registered address.

3.4.5.3 The asset registration company may supply additional information about the asset and registered keeper to law enforcement officers if:

(a) the asset to which the details relate is registered as lost or stolen
(b) the information is supplied to the enquirers registered address and that address is recognised as being a police station or other such law enforcement office, and
(c) the registered keeper has agreed to the information being supplied to law enforcement officers or the asset registration company is otherwise required by law to release that information.

3.4.5.4 The asset registration company shall not provide anyone other than the registered keeper or law enforcement officer's access to any secure information about the assets or keepers stored on grade 2, 3 or 4 secure asset registers other than that information covered in clauses 3.4.5.2 and 3.4.5.3.

3.4.5.5 The asset registration company may provide access to information about the assets or confirm the keeper's details stored on grade 1 secure asset registers to enquirer's other than the associated registered keeper or law enforcement officers if:

(a) the enquirer has appropriate access privileges, including permission from the registered keeper that the information may be supplied to that enquirer, and
(b) the information is sent to the enquirer's registered postal address.

3.4.5.6 When transmitting secure information by post, all of the requirements contained in Table 5 shall be met.

Table 5 Minimum requirements for transmission of secure information by post

Clause	Requirement	Grade			
		1	2	3	4
3.4.5.6.1	Secure information shall only be sent to the enquirers registered postal address	Y	Y	Y	Y
3.4.5.6.2	The recipients contact details placed on the package containing the secure information shall be checked to ensure it is correct before despatch	Y	Y	Y	Y
3.4.5.6.3	Only authorised couriers complying with the relevant requirements of this standard shall be used	R	R	Y	Y
3.4.5.6.4	Secure information shall is transmitted in tamper-evident packaging that will protect the contents from any environmental conditions the package can reasonably be expected to encounter between dispatch and receipt. *Note: Requirements relating to the transmittal of passwords by post are contained in clause 3.4.8.11.*	R	R	Y	Y
3.4.5.6.5	Auditable transmittal details shall be recorded and shall include: • courier details • dispatch date • dispatcher • collector • receipt date • addressee who received the item and when	R	R	Y	Y
Key:	R = Recommended Y = Requirement				

3.4.6 Exchange of secure information by facsimile

3.4.6.1 Any designated facsimile machine used to receive enquiries or registration details shall be located within secure areas.

3.4.6.2 The asset registration company may fax a 'yes'/'no' answer to the question "Is asset '####' registered as lost or stolen?" (where #### is the asset registration number marked on the asset) to a general enquirer.

3.4.6.3 The asset registration company may fax a 'yes'/'no' answers to the question "Is 'x' the registered keeper of asset '####'?" (where #### is the asset registration number marked on the asset) to an enquirer providing:

(a) the enquirer has appropriate access privileges, and
(b) the fax number to which the answer is the sent is the registered fax number for that enquirer, and
(c) a system of checking the fax number is implemented to ensure details are not sent to an incorrect fax number.

3.4.6.4 The asset registration company may supply additional information about the asset and registered keeper of assets on grade 1 and 2 secure asset registers to law enforcement officers by facsimile if:

(a) the asset to which the details relate is registered as lost or stolen
(b) the information is supplied to the enquirers registered fax number and that fax number is recognised as being in a police station or other such law enforcement office, and
(c) the registered keeper has agreed to the information being supplied to law enforcement officers or the asset registration company is otherwise required by law to release that information.

3.4.6.5 The asset registration company shall not send any secure information by facsimile unless that is not covered in clauses 3.4.6.2, 3.4.6.3 and 3.4.6.4 by facsimile.

3.4.7 Information access control

3.4.7.1 Access to the information held on the secure asset register and electronic security systems designed to protect that information (e.g. access control systems and network operating systems) shall be restricted by means of user identification, and access shall only be granted to registered users and operators with appropriate access privileges.

3.4.7.2 User and operator registration and de-registration procedures shall exist.

3.4.7.3 All appropriate requirements of clauses 3.3.3 and 3.3.4 shall be met before registering operators.

3.4.7.4 All users shall be given a written statement of access privileges and be required to either sign an appropriate set of terms and conditions (if applying for access by post, fax or in person) or indicate their acceptance of a set of terms and conditions (if registering via internet).

The terms and conditions of access shall cover the requirements of clause 3.4.8.13.

No access privileges shall be granted without their acceptance of the terms and conditions of access.

3.4.7.5 Each registered user and operator shall be issued with a unique identifier (user ID)* and password, in accordance with clause 3.4.8. Grade 3 and 4 secure asset registers shall require the use of at least two passwords, one of which may take the form of an answer to an open question.

**Note: The use of alternative means of computer access control, such as fingerprint recognition, is permitted.*

3.4.7.6 Access privileges shall limit the person to whom they are issued to only undertaking those operations (privileges) they are authorised to carry out, as defined in the information security management system and Table 6.

Table 6 Access privileges

Operation	**Operator (0) / System administrator (A)**	**Registered keeper**	**General user**	**Law enforcement officer**
Setting up a user account	0 (1)	Y	Y	Y
Registering details of assets on the secure asset register	0 (1)	Y	Y	Y
Editing user information	0 (1)	Y (2)	Y (2)	Y (2)
Editing asset information	0 (1)	Y (2)	Y (2)	Y (2)
Reporting the loss or theft of assets	0 (1)	Y	N	Y
Reporting the finding/retrieving of assets previously reported as lost of stolen	0 (1)	Y	Y	Y
Obtaining a 'yes'/'no' answer to the question "Is asset '####'(3) registered as lost or stolen?"	0 (1)	Y	Y	Y
Obtaining a 'yes'/'no' answer to the question "Is 'x' the registered keeper of asset '####'(3)?"	0 (1)	Y (2)(4)	Y (4)	Y (4)
Obtaining access to all the information registered in relation to an asset except for the registered keepers user ID and password(s)	0 (1)	Y (2)	N	Y (4)
Access to database operating system and/or database source code.	A (5)(6)	N	N	N
Access to servers used to store/process the information held on the secure asset register	A (6)	N	N	N
Setting operator and administrator privileges and system access rules	A (5)(6)	N	N	N

Key	Y = Yes N = No 0 = Operator A = System administrator
Notes	(1) On behalf of the relevant registered keeper, user or law enforcement officer only. (2) Information relating to their own account only. (3) '####' indicates the asset registration number marked on the asset. (4) The registered keeper shall have first given their permission for that enquirer to be given access to that level of information, or the asset register is otherwise required by law to release that information. (5) The number of system administrators with the privileges to undertake these operations shall be kept to a minimum. (6) These operations shall require "double key access" on grade 2, 3 and 4 systems, that is, confirmation by another authorised operator.

3.4.7.7 A person's access privileges shall be immediately suspended if it becomes known their password is in any way compromised, and a new password(s) issued.

3.4.7.8 A person's access privileges shall be immediately terminated if:
(a) Their status changes, and that change undermines the person's compliance with all relevant requirements of this standard.
(b) They break the terms and conditions of access.

3.4.7.9 A nominated management representative shall verify the effective suspension and/or termination of access privileges.

3.4.7.10 The issue, suspension and termination of access privileges shall be recorded and a periodic review of access privileges conducted to ensure it is accurate and up to date.

3.4.8 User IDs and passwords

3.4.8.1 User IDs and passwords shall comply with the requirements defined in Table 7.

3.4.8.2 Users wishing to set or change their password for electronic access to the secure information shall be required to enter their desired password(s) twice and the system shall reject the application to set/change the password if the two passwords entered do not match.

3.4.8.3 Each system administrator shall be assigned a unique user ID and password(s) which shall be entered in order to permit them to undertake system administration functions. Those user IDs and passwords shall comply with clauses 3.4.8.1 and 0.

3.4.8.4 Passwords shall not contain the associated user ID.

3.4.8.5 Passwords used on grade 3 and 4 secure asset registers shall be one way encrypted.

3.4.8.6 The characters of the password entered onto the system by the user shall not be displayed in plain text or be disclosed by audible feedback.

3.4.8.7 Redundant user IDs shall not be issued to other users.

3.4.8.8 Users registering for access to the secure asset register via the internet shall also register their email address. This shall be the email address to which access privileges are confirmed and, should the user forget their password or user ID, reminders are sent. The system shall require the email address to be entered twice and shall reject the application for registration if the two email addresses entered to do not match.

3.4.8.9 No procedure shall require or permit oral communication of the password(s), either by telephone or in person.

Table 7 Minimum user ID and password requirements

Grade		**1**	**2**	**3**	**4**
User ID	Minimum number and type of characters	8 digits made up of any of the following: Uppercase letters Lower case letters Numbers Special characters	As per grade 1.	As per grade 1.	As per grade 1.
	Generation	Defined by asset registration company. The user ID may take the form of the users email address.	As per grade 1.	Defined by asset registration company. The user ID shall not take the form of the users email address.	As per grade 3.
Primary Password	Minimum number and type of characters	8 digits containing at least two of the following: • Uppercase letters • Lower case letters • Numbers	8 digits containing at least three of the following: • Uppercase letters • Lower case letters • Numbers • Special characters	As per grade 2.	10 digits containing at least three of the following: • Uppercase letters • Lower case letters • Numbers • Special characters
	Generation	User defined[(a)]	User defined[(a)]	User defined[(a)]	User defined[(a)]
Secondary Password	Minimum number and type of characters	None	None	As per requirements for primary password.	As per requirements for primary password.
	Generation	None	None	User defined	User defined

Notes:

(a) The system may automatically generate the primary password. This shall be unique to that user and shall not be based on any information provided by the user or the content of the user ID. Grade 3 and 4 secure asset registers shall require the user to change automatically generated passwords when they first log on.

(b) A password management system may be used to ensure the user ID's and passwords used to access the secure information and to confirm administrator rights comply with requirements defined in this table and clause 3.4.8.4.

3.4.8.10 At no point in the delivery process shall the password appear in plain text if it can be associated with a user's account unless the password is sent by:

(a) Secure encrypted email to the email account registered by that user. If it is sent by this means, the password shall not appear within the email subject or address lines.

(b) Post.

3.4.8.11 Passwords issued by post shall be sent in an envelope or other container that:

(a) prevents the password being read without opening the envelope/container, and
(b) protects the password against degradation until the envelope/container is opened, and
(c) is tamper evident.

The password shall be accompanied by a warning to the user advising them not to use the password if there is evidence its security may have been compromised and to immediately notify the asset registration company.

3.4.8.12 Passwords giving access to grade 3 and 4 secure asset registers that are issued by post shall be sent by recorded delivery. An auditable record of transmission shall be retained in accordance with clause 3.2.7 and shall include:

- courier details
- dispatch date
- dispatcher
- collector
- receipt date
- addressee
- who received the item and when.

3.4.8.13 All users and operators shall be advised of their responsibilities in relation to the security of their user ID and passwords. This shall include:

(a) Keeping passwords confidential.
(b) Not sharing their password and user ID or access to the secure asset register with others.
(c) Not using the same password they use for other purposes (e.g. personal banking).
(d) Changing passwords if they believe they may have been compromised and the need to advise the asset registration company.
(e) Not using automated logging-on facilities that automatically enter the user ID and/or password(s).
(f) Not leaving equipment that is logged-on to the secure asset register unattended.

All users and operators shall be required to indicate their acceptance of these responsibilities before being granted access privileges and this shall be recorded by the asset registration company.

3.4.8.14 Operators and users shall be required to change their passwords periodically.

The maximum time operators and users shall be permitted to retain each password is defined in Table 8.

Operators and users shall not be permitted to set their password as one which they have had as one of their last eight passwords for that secure asset register.

3.4.8.15 Users and operators access privileges shall be cancelled if they exceed three consecutive incorrect user ID and/or password entries.

Table 8 Maximum password retention periods

Grade	Operators and administrators	Users
1	12 months or until access privileges are terminated	Until access privileges terminated*
2	6 months or until access privileges are terminated	Until access privileges terminated*
3	3 months or until access privileges are terminated	12 months or until access privileges are terminated
4	1 month or until access privileges are terminated	6 months or until access privileges are terminated

**Note: It is recommended that users be advised to change their password at least every 12 months.*

3.4.8.16 All incorrect access attempts shall be recorded in accordance with clause 3.2.10.1.

3.4.8.17 A procedure for reissuing forgotten passwords or user IDs shall be developed and implemented. Confirmation of a forgotten password shall only be issued to the postal or email address registered on the secure asset register and shall be communicated in accordance with the requirements for issuing passwords defined in the following clauses:

Method by which the password is issued	Relevant clauses of this standard
Post	3.4.8.10, 3.4.8.11 and 3.4.8.12.
Email	3.4.8.10.

3.4.8.18 Users with internet access wishing to change their password shall be required to first access the system by entering their current user name and passwords. They shall then be required to input their desired password(s) twice. The system shall reject their application to change the passwords if each pair of passwords entered does not match.

3.4.9 Managing other sources of secure information

3.4.9.1 All documents relating specifically to information stored on the secure asset register or the control of access to the secure asset register shall be protected from unauthorised viewing. These include completed registration forms, hard copies of the secure asset register contents and password lists.

Note: It is recommended that asset registration companies consider storing secure information in storage devices conforming to the security standards noted in

Table 9 Minimum recommended security performance of document storage cabinets

Grade	*Minimum recommended security performance of document storage cabinet according to the standards against which those storage devices are approved.*			
	LPS 1228	*EN 14450*	*LPS 1175*	*LPS 1183 or EN 1143-1*
1	*1*	*S1*	*SR1*	*0*
2	*1*	*S1*	*SR1*	*0*
3	*3*	*S2*	*SR2*	*0*
4	*4*	*S2*	*SR3*	*0*

3.4.9.2 The issue and use of removable computer media such as discs, tapes, printed reports and printer ribbons from the asset registration company shall be controlled and documented.

3.4.9.3 Any media containing secure information stored on the secure asset register or that can be used to access the secure information stored on the secure asset register shall be protected against unauthorised access if transported outside the secure areas defined within clause 3.3.2.1. Any media that is transported outside of the secure areas shall be accompanied by transmittal notices and copies of those notices retained.

3.4.9.4 Computer media and all security sensitive documents shall be securely disposed of when no longer required.

3.4.9.5 Secure information shall be permanently erased from all hardware prior to disposal.

Note: Guidance on techniques for ensuring secure information is erased from ICT equipment is contained in Annex G of BS EN 29564-1:1994 Banking - Personal Identification Number management and security - Part 1: PIN protection principles and techniques

3.4.9.6 The disposal of computer media and security sensitive documents shall only be undertaken by authorised personnel or contractors in accordance with BS 8470: 2006 *Secure destruction of confidential material - Code of practice*, and shall be recorded.

3.4.9.7 Printers used to generate documents containing registered keeper's details, for example, registration confirmation slips, shall be located within a secure area and shall only be accessible to those authorised to have access to the secure information.

3.4.9.8 The use of photocopiers, fax machines, cameras and other imaging/copying devices shall be managed to prevent the unauthorised copying of secure information.

3.4.9.9 No access to the secure information shall be given when demonstrating the secure asset register's functionality and capability to potential users unless the person to whom the secure asset register is being demonstrated has provided that information. This does not preclude the use of dummy information placed on the secure asset register purely for the purpose of demonstrating and testing the secure asset register.

3.5 Asset registration and enquiry processing

3.5.1 Asset registration

3.5.1.1 The asset registration company shall ensure that the following details relating to the assets registered on the secure asset register are recorded on the secure asset register:

(a) The title (e.g. Mr, Mrs, Miss, Ms), full name, full address (including postcode) and contact telephone number of the person registering the asset.
(b) The email address of the person registering the asset, if that person requires access to their account via the internet or wishes to receive their access user name and password.
(c) The title (e.g. Mr, Mrs, Miss, Ms), full name, full address (including postcode) and contact telephone number of the person to be registered as the keeper of the asset, if different from (a).
(d) The relationship of the person registering the asset to the registered keeper of the asset (e.g. supplier (if registered by the person supplying a marked asset), insurer, hirer/finance company (if the asset is leased to a third party))
(e) The type of asset (e.g. make, model).

3.5.1.2 The asset registration company shall also request the following information from those registering the assets:

(a) Details of any asset marking device(s) present on the asset and asset identification code(s) to be found on the asset marking device(s).
(b) The type and content of other codes present on the asset which may help to identify the asset (e.g. serial codes, batch numbers).

3.5.1.3 Secure asset registers that may be used to record assets which are unlikely to be marked using asset marking devices shall include the option for those registering the asset to submit one or more photographs of that asset.

Note: Asset registration companies should also consider asking those registering assets to provide a description of the asset and other information that can be used to identify the asset, for example the age, colour(s), weight, dimensions and distinguishing marks.

3.5.1.4 Confirmation of asset registration shall be sent to the registered keeper and the person registering the asset (if different) by one or more of the following methods:

- Emails to the registered keeper(s) via the email addresses provided by the new and previous registered keeper. These emails shall comply with the requirements of clause 3.4.4.
- Post to the postal address provided by the registered keeper(s). This shall comply with the requirements of clause 3.4.5.
- Provision of access to information via the internet. This shall comply with the requirements of clause 3.4.3.

3.5.2 Updating asset status

3.5.2.1 The asset registration company shall provide a mechanism by which registered keepers can confirm the transfer of ownership/keepership of a registered asset to another person. These shall comply with the requirements of clause 3.4 relevant to the methods of information exchange accommodated by the secure asset register.

3.5.2.2 Registration shall only be transferred to a new registered keeper on receipt of confirmation of the transfer from the previous registered keeper* and registration of the asset by the new registered keeper in accordance with clause 3.5.1.

**Note: Exceptions to this clause may occur where the previous registered keeper is known to have died or where the new keeper can provide appropriate evidence that ownership has transferred to them.*

Asset registration companies should consider keeping a record of all previous registered keepers of an asset as this could aid investigations by law enforcement officers. However, registered keepers should agree to such records being maintained and current/subsequent registered keepers shall not have access to those details other than as covered in clause 3.4.

3.5.2.3 The asset registration company shall provide a mechanism by which registered keepers can confirm if any of the following events occur:

(a) The asset is lost or stolen. This shall include facilities to provide information relating to the following:
   - The lost property reference/crime number
   - The police station or other location at which the loss/theft was reported
   - The date on which the loss/theft was reported

(b) Assets registered as lost or stolen are subsequently found.

(c) The asset's characteristics are changed in any way that may affect the information used to describe the asset on the secure asset register.

(d) The asset is destroyed or disposed of.

(e) The registered keeper wishes to cancel their registration on the secure asset register.

3.5.2.4 Notification of change of ownership or change of status received by telephone and fax and email shall only be permitted on grade 1 and 2 databases and then only

when the identity of the person notifying the secure asset register of the changes has been verified.

Note: This may be achieved by asking the person to:
- *provide a previously notified pass phrase*
- *correctly answers a series of security questions (common examples include date of birth and mother's maiden name).*

3.5.2.5 The asset registration company shall validate the identity of the person claiming to be the registered keeper before recording a change of ownership or change to product status.

Note: One way to achieve this is by requesting the registered keeper to input their correct user ID and password(s) when submitting the request online.

3.5.2.6 The asset registration company shall confirm changes to the ownership/status of an asset or notification of theft/loss of an asset by one or more of the following methods:
- Emails to the registered keeper(s) via the email addresses provided by the new and previous registered keeper. These emails shall comply with the requirements of clause 3.4.4.
- Post to the postal address provided by the registered keeper(s). This shall comply with the requirements of clause 3.4.5.
- Provision of access to information via the internet. This shall comply with the requirements of clause 3.4.3.

Note: Any confirmation of change of ownership sent to the previous registered keeper shall only confirm that the registration has transferred and the asset registration number(s) or other unique identifier(s) of the asset(s) being transferred.

3.5.3 Data entry validation

3.5.3.1 A system of information entry checking shall be in place to check the information placed on the secure asset register reflects that provided by the user.

If the asset registration company enters information on behalf of the customer, those entries shall be checked using the information supplied by the customer.

If the information is entered directly by the customer, the system shall automatically check the information to ensure that all relevant fields are completed and that the information format complies with that required within those fields.

3.5.3.2 The following information validation checks shall be incorporated within the secure asset register and shall be set to suit the information being validated:
(a) Out-of-range values
(b) Invalid characters in data fields
(c) Missing or incomplete information
(d) Exceeding upper or lower data volume limits

3.5.3.3 The asset registration company shall have defined procedures for processing unclear and incomplete information. At minimum, these shall define the procedures for obtaining the following from the person registering the asset:
(a) missing/incomplete information
(b) the content of any unclear information.

3.5.3.4 Regular audits of the information validation processes shall be conducted to ensure the information validation is working effectively.

4 MARKING, LABELLING AND PACKAGING

Documents relating specifically to the secure asset register assessed by the LPCB shall be marked with the asset registration company's trade name and trademarks under which the secure asset register is approved to this standard.

5 PUBLICATIONS REFERRED TO:

BS 7858: 2006	Security screening of individuals employed in a security environment - Code of practice
BS 7950: 1997	Specification for enhanced security performance of casement and tilt/turn windows in domestic applications
BS 8470: 2006	Secure destruction of confidential material - Code of practice
BS 8418: 2003	Installation and remote monitoring of detector activated CCTV systems. Code of practice
BS 25999-1:2006	Business continuity management. Part 1: Code of practice
BS EN 1143-1: 2005	Secure storage units. Requirements, classification and methods of test for resistance to burglary. Safes, ATM safes, strongroom doors and strongrooms
BS EN 14450: 2005	Secure storage units. Requirements, classification and methods of test for resistance to burglary. Secure safe cabinets
BS EN 29564-1:1994	Banking - Personal Identification Number management and security - Part 1: PIN protection principles and techniques *(also published as ISO 9564-1: 1991)*
BS EN 50131-1: 2006	Alarm systems. Intrusion and hold-up systems. System requirements
ISO 9001	Quality management systems. Requirements

BS ISO/IEC TR 13335-3: 1998	Information technology - Guidelines for the management of IT Security - Part 3: Techniques for the management of IT security
BS EN ISO/IEC 17021:2006	Conformity assessment. Requirements for bodies providing audit and certification of management systems
BS ISO/IEC 18043: 2006	Information technology. Security techniques. Selection, deployment and operations of intrusion detection systems
BS ISO/IEC 27001: 2005	Information technology - Security techniques - Information security management systems - Requirements *(BS 7799-2: 2005)*
LPS 1175: Issue 6	Requirements and testing procedures for the LPCB approval and listing of intruder resistant building components, strongpoints, security enclosures and free-standing barriers
LPS 1183: Issue 4	Requirements and testing procedures for the LPCB approval and listing of safe storage units
LPS 1225: Issue 3	Requirements for the LPCB approval and listing of asset marking systems
LPS 1228: Issue 1	Specification for testing and classifying the burglary resistance of office furniture – lightweight containers
LPS 1269 *(draft)*	Specification for testing and classifying “microdot” asset marking devices
LPS 1650: Issue 1	Requirements and testing procedures for the LPCB approval and listing of ‘theft resistant’ electronic products
LPS 1651 *(draft)*	Requirements for the LPCB Approval and listing of ‘forensic’ asset marking systems
PAS 24-1: 2007	Enhanced security performance requirements for door assemblies. Single and double leaf, hinged external door assemblies to dwellings
PD ISO/IEC TR 18044: 2004	Information technology - Security techniques - Information security incident management

For undated references please refer to the latest published issue.

Amendments Issued Since Publication

DOCUMENT NO.	AMENDMENT DETAILS	SIGNATURE	DATE
LPS 1224-3.1	1. New front cover 2. Title added to header 3. Notes amended on Page 4 4. Repagination 5. Update to copyright information 6. Update of references to ISO 9001 standard (Clauses 2, 3.1, 3.2, 3.3 & 5)	DC	Jan. 2014