

DIGITAL RECORDS ACCESS CONTROL POLICY

Project name	Seamless Flow: Management and Security
Release	Date: July 2005
Author:	Project Manager
Owner:	Senior Responsible Owner (SRO)
Client:	The National Archives (TNA)

1. Document History

Document This document is only valid on the day it was printed.
 Location The source of the document will be found in the Quality File.

Revision date	Version	Summary of Changes	Changes marked
May 2005	0.1	First draft	NO
Jun 2005	0.2	Small changes to clarify the text	NO
July 2005	0.3	Added annex describing security levels and comparison method.	NO

Approvals This document requires the following approvals.
 Signed approval forms are filed in the project files.

Title	Date of Issue	Version
SRO		
Programme Manager		

Distribution This document has been distributed to:

Title	Date of Issue	Version
SRO	13 Jul 2005	0.3
Programme Manager	13 Jul 2005	0.3
Project manager for public web search	13 Jul 2005	0.3
Head of Records Management Department	13 Jul 2005	0.3
Management and Security project team	13 Jul 2005	0.3
Seamless Flow project managers	13 Jul 2005	0.3

2. Contents

1. Document History	1
2. Contents	2
3. Digital Records Access Control Policy	3
3.1. Terminology	3
3.1.1. <i>Indicating requirement levels.....</i>	3
3.1.2. <i>Access control terminology.....</i>	3
3.1.3. <i>Document references.....</i>	3
3.1.4. <i>Digital records terminology.....</i>	3
3.1.5. <i>Seamless Flow programme terminology.....</i>	3
3.2. Executive Summary	4
3.2.1. <i>Policy summary.....</i>	4
3.2.2. <i>Compliance</i>	4
3.3. Policy.....	5
3.3.1. <i>Authentication.....</i>	5
3.3.2. <i>No unauthorised information flow from a higher to a lower level.....</i>	5
3.3.3. <i>Preserve integrity.....</i>	6
3.3.4. <i>Manage access control securely</i>	6
3.3.5. <i>Audit of access requests and changes</i>	7
3.3.6. <i>Well-formed transactions</i>	7
3.3.7. <i>Separation of duties</i>	8
3.3.8. <i>Principle of least privilege.....</i>	8
3.3.9. <i>Minimising the attack surface</i>	8
3.3.10. <i>Block access to the layer below</i>	8
3.3.11. <i>Defence in depth</i>	8
4. Annex A.....	9
4.1. Document References	9
4.1.1. <i>TNA Security Policy.....</i>	9
4.1.2. <i>The Manual of Protective Security.....</i>	9
4.1.3. <i>Corporate ISMS Policy (BS7799-2).....</i>	9
4.1.4. <i>Requirements for Electronic Records Management Systems 2002, final draft</i>	9
4.1.5. <i>GSI accreditation requirements</i>	10
4.1.6. <i>RFC2119 – Indicating requirement levels</i>	10
4.1.7. <i>SF-MS-TERMI – Digital Records Terminology</i>	10
4.1.8. <i>Seamless Flow Programme Glossary</i>	10
4.1.9. <i>Clark Wilson - a comparison of commercial and military security policies</i>	11
4.1.10. <i>Bell LaPadula – Secure Computer System: unified exposition.....</i>	11
4.2. Document Glossary	12
4.2.1. <i>Access control terminology.....</i>	12
5. Annex B.....	15
5.1. Protective markings.....	15
5.1.1. <i>Unclassified records</i>	15
5.1.2. <i>Restricted records</i>	15
5.2. Security levels	16
5.2.1. <i>Visualising security levels.....</i>	16
5.2.2. <i>Comparing security levels.....</i>	17
5.2.3. <i>Access control examples</i>	18

3. Digital Records Access Control Policy

3.1. Terminology

3.1.1. Indicating requirement levels

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119]

3.1.2. Access control terminology

Terms introduced by this document are defined in the **Document Glossary**. In order to provide context, each term is also introduced in the relevant section of the policy to which they are most applicable.

Particularly note that the words **subject** and **object** are used in this document in a formal computer security sense, not necessarily as they may be used other parts of the Seamless Flow programme:

Subject The active entity in an **access control decision**, the requestor of **access rights** to an **object**. A subject may be a user, or it may be a process running on a computer.

Object The passive entity involved in an **access control decision**; the thing to which a **subject** requests **access rights**.

3.1.3. Document references

Words in [**bold**] also enclosed in square brackets are **Document References**.

3.1.4. Digital records terminology

Concepts relating to digital records in this document are taken from above paper

3.1.5. Seamless Flow programme terminology

Other terms used in the Seamless Flow programme are defined in the glossary

3.2. Executive Summary

The digital records held by the National Archives are irreplaceable and require protection indefinitely. This document defines an access control policy¹ designed to meet the security requirements² of these information assets.

3.2.1. Policy summary

For all digital records and supporting systems, it is a requirement to:

- (1) Allow no unauthorised information flow from a higher to a lower level
- (2) Preserve integrity over very long periods of time
- (3) Manage access control securely
- (4) Maintain an audit log of access requests and changes

In support of these requirements, there shall be:

- (5) Well-formed transactions
- (6) Separation of duties

These general access control principles shall be applied in support of the policy:

- (7) Principle of least privilege
- (8) Minimising the attack surface
- (9) Block access to the layer below
- (10) Defence in depth

3.2.2. Compliance

The digital records access control policy is aligned with:

- (1) TNA Security Policy
- (2) The Manual of Protective Security
- (3) TNA Corporate Information Security Management System
- (4) Requirements for Electronic Records Management Systems 2002
- (5) GSI accreditation requirements
- (6) Clark-Wilson – a comparison of commercial and military policy
- (7) Bell LaPadula – secure computer systems

¹ This document is only concerned with defining logical access control policy for digital records and supporting systems and metadata. Further documents will precisely define a logical access control model and specify a technical implementation consistent with our infrastructure if appropriate.

² Security controls other than logical access control are required to fully secure the records, including, but not limited to, physical access control, intrusion detection and network controls, change management, business continuity planning and disaster recovery procedures.

3.3. Policy

Any object to which access is controlled by this policy shall be termed a **controlled object**.

Controlled objects that are:

- (1) Intended to be publicly available to read by some method (even if some restrictions apply) shall be termed **open material**.
 - a. Open material for which there exists no explicit restriction on public read access shall be termed **fully open material**.
 - b. Open material for which there exists some explicit restriction on public read access shall be termed **partially open material**.
- (2) Not intended to be publicly available by any method shall be termed **closed material**.

3.3.1. Authentication

- (1) Subjects must be subject to **strong authentication** if they:
 - a. Access **closed material**.
 - b. Have an **editorial role**.
 - c. Have a **permissions role**.
- (2) The strength of the authentication process must conform to government security policy for access to the security classification of the controlled object.

3.3.2. No unauthorised information flow from a higher to a lower level

A right to read a controlled object shall be termed a **read right**. If a security level³ is equal to or greater than another, the former is said to **dominate**⁴ the latter.

- (1) No read up - in order for a subject to be granted a read right to a controlled object, the security level of the subject must dominate the security level of the controlled object⁵.
- (2) No write down – subjects shall not copy information from a controlled object to a controlled object of a lower security level⁶.

By default, all subjects have read rights to controlled objects, which are presumed to be fully open material unless explicitly restricted – control by explicit restriction. This constitutes a mandatory access control policy for record confidentiality.

³ Note that a security “level” may not be a simple linear classification, such as Unclassified, Restricted, or Classified. It can accommodate a complex, multi-dimensional structure, for example, also allowing for the control of Freedom of Information, Sensitivity and Copyright, by the assignment of sets of security labels to subjects and objects.

⁴ The precise mathematical rules for comparison of complex security levels are given in **Annex B**.

⁵ This is in accordance with the “ss” property of the government confidentiality model, Bell LaPadula [**BLP76**].

⁶ This is a simplified version of the [**BLP76**] “*” security property, designed to prevent downwards information leakage. It is presented as a behavioural directive, rather than a formally enforceable constraint. It is extremely hard to technically enforce the * property using modern commercial operating systems, although systems and applications should seek to enforce this rule as far as possible. Further controls are required to mitigate this type of malicious attack, including secure audit of changes.

3.3.3. Preserve integrity

Rights that allow the creation, modification or destruction of a controlled object shall be termed an **editorial right**. Any role with an editorial right shall be termed an **editorial role**.

- (1) An editorial role must have a clearly defined purpose.
- (2) An editorial role must be limited to the minimum access rights required for its purpose.
- (3) The allocation of editorial roles to user accounts shall be kept to a minimum⁷.

By default, no subject has any editorial rights; they must be explicitly assigned to roles and the roles to the users – control by explicit permission. This constitutes a discretionary access control policy for record integrity⁸.

There are two further mandatory components to complete the integrity policy:

- (4) Editorial rights shall not be granted unless the subject also has a read right to the object.
- (5) All editorial access to controlled objects shall be well formed⁹.

3.3.4. Manage access control securely

In order to maintain the security of the digital records, it is essential to control the process of allocating rights to subjects and of changing the security levels of controlled objects.

- (1) Access rights must not be allocated directly to subjects; specific access rights shall be allocated to defined roles¹⁰, and roles then allocated to subjects.

A right to create or delete roles, change editorial or execute rights for a role, or assign roles to subjects, shall be termed a **permissions right**. Any role with a permissions right shall be termed a **permissions role**.

- (2) A permissions role must only have permissions rights allocated to it.

An editorial right that permits a change to the security level¹¹ of a controlled object shall be termed a **restriction right**. An editorial role with a restriction right shall be termed a **restriction role**.

- (3) A restriction role must only have restriction rights allocated to it.

These roles shall be separated in accordance with the requirement of **Separation of duties**.

⁷ In the case where a user appears to require several editorial roles, the possibility of splitting the job function shall be considered.

⁸ This policy is in accordance with the integrity policy described by Clark and Wilson in [CLARKWILSON]

⁹ See 3.3.6 – Well-formed transactions.

¹⁰ Role based access control simplifies security management and allows for quick and easily reversible assignment of additional rights to another user, for example, when a member of staff is away.

¹¹ For example, by modifying Classification, Sensitivity, Copyright, or Freedom of Information metadata.

3.3.5. Audit of access requests and changes

- (1) All changes to editorial, permission and execute roles, or their allocation to subjects shall be audited.
- (2) All access requests by a subject for editorial, permission and execute rights shall be audited.
- (3) All access request failures shall be audited.
- (4) Any creation, modification, or destruction of a controlled object by a subject shall be audited
- (5) Audit logs are themselves controlled objects and shall be protected from unauthorised observation, modification or deletion.
- (6) Audit logs shall carry the maximum security level of the information audited.

3.3.6. Well-formed transactions

It is essential to ensure that information in a system possesses **internal integrity**. By controlling access to information through certified functions or applications, it is possible to ensure that the information remains in a validated, self-consistent state.

An application or function that can create, modify or delete a controlled object shall be termed a **transformation procedure**.

Input to a transformation procedure shall be termed an **unconstrained data item**. Output of a transformation procedure shall be termed a **constrained data item**.

An application or function that provides internal integrity verification of a constrained data item shall be termed an **integrity verification procedure (IVP)**

A right to execute a transformation procedure shall be termed an **execute right**. A role with an execute right shall be termed an **execute role**.

By default, no subjects shall have execute roles – control by permission.

- (1) Transformation procedures shall be certified as being correct.
- (2) Access to execute transformation procedures shall be limited to defined execute roles.
- (3) Editorial access to controlled objects shall only be through transformation procedures¹².
- (4) Transformation procedures shall validate unconstrained data items, and if validation fails shall reject the input. Validated input becomes a constrained data item.
- (5) Integrity verification procedures shall verify the ongoing integrity of constrained data items.

¹² The ideal scenario is one in which a user has no explicit rights to controlled objects, but only has execute rights to run a particular set of transformation procedures. The transformation procedure then runs with an editorial role, allowing it to make validated changes, but preventing a user from directly modifying a controlled object. For example, this type of control can be seen in relational databases, or other client-server applications.

In cases where it is not possible to technically enforce this policy constraint (for example, where a stand-alone application is editing an XML file), it may be desirable to create a means for its integrity verification procedure to detect unauthorised changes made to the constrained data items outside the control of the transformation procedure.

3.3.7. Separation of duties

It is essential to ensure that information in a system possesses **external integrity**. By separating the duties of subjects who have access to the information, the risk of both accidental and malicious damage may be mitigated.

- (1) A subject allocated a permissions role must not have an editorial or execute role.
- (2) A person who certifies a transformation procedure must not have execute rights to it.

The rules above form only a minimum separation of duties. In practice, privileges within the defined role categories may be further sub-divided¹³ according to requirements and in line with the **Principle of least privilege**.

3.3.8. Principle of least privilege

The principle of least privilege requires that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. Application of this principle limits the damage that can result from accident, error, or unauthorized use of an information system.

- (1) All processes, systems, applications and networks to which this policy applies shall apply the principle of least privilege.

3.3.9. Minimising the attack surface

Attack surfaces are the number of routes by which an attack can flow. This can include, but is not limited to network services, locally installed applications, and file system access control permissions.

- (1) All processes, systems, applications and networks to which this policy applies shall minimise the attack surface presented to a potential attacker.

3.3.10. Block access to the layer below

An attacker gaining access to a layer below the layer at which controls are applied may frequently bypass those controls¹⁴.

- (1) All processes, systems, applications and networks to which this policy applies shall block access to any layer below the level of the control.

3.3.11. Defence in depth

- (1) Access controls should be implemented at as many layers as is practical and cost-effective¹⁵.

¹³ For example, an editorial role with the right to create a controlled object is likely to be separate from one that may destroy a controlled object.

¹⁴ Examples of gaining access in this way include not protecting backup tapes to the same degree as the information in the live system, using a low level disk-reading tool to read the data on a disk directly, thus bypassing logical system access controls, or editing an XML document with a text editor instead of using the certified transformation procedure.

¹⁵ For example, an application may directly restrict who may edit a document, and the operating system may also enforce similar file access permissions on the document. It is not necessary for controls to provide equivalent protection at each layer. It is likely that some layers will only be able to implement the access control policy partially, but which in combination provide useful policy support and risk mitigation.

4. Annex A

4.1. Document References

4.1.1. TNA Security Policy

The TNA Security Policy [TNASecPol] gives the overarching security policy for the National Archives. It can be found in the National Archives file plan at:

```
/Information and Communication Technology
  /Projects /Seamless Flow - Management and Security
    /Resources /Information Security /TNA
      /TNA Security Policy
```

4.1.2. The Manual of Protective Security

The Manual of Protective Security [MPS] is a security manual broadly building on ISO17799 providing specific guidance on protecting information assets for the UK government. It is a Restricted document; permission must be sought from the Departmental Security Officer to obtain a copy.

4.1.3. Corporate ISMS Policy (BS7799-2)

The Information Security Management System [BS7799-2-ISMS] defines how we comply with BS7799 at the National Archives. It can be found in the National Archives file plan at:

```
/Information and Communication Technology
  /Projects /Seamless Flow - Management and Security
    /Resources /Information Security /TNA
      /Corporate ISMS Policy Statement
```

4.1.4. Requirements for Electronic Records Management Systems 2002, final draft

The Requirements for Electronic Records Management Systems 2002 [ERMS-REQ-2002] defines access control requirements for electronic records management systems.

While the systems within the Seamless Flow programme are not ERM systems themselves, they have a clear relationship with them, as they too are involved with the management of electronic government records. The digital records access control policy has been informed by this document and is compatible with it. It can be found at:

<http://www.nationalarchives.gov.uk/electronicrecords/reqs2002/pdf/requirementsfinal.pdf>

4.1.5. GSI accreditation requirements

Systems on the GSI network require accreditation to information security standards laid out by the Codes of Connection to the GSI network. Please ask the ICT department for details of accreditation to GSI. [**GSI-REQ**]

4.1.6. RFC2119 – Indicating requirement levels

[**RFC2119**] defines the keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" to allow the precise indication of requirement levels where there may be security implications.

It can be found on the Internet at:

<http://www.faqs.org/rfcs/rfc2119.html>

Or alternatively in the National Archives file plan at:

```
/Information and Communication Technology
  /Projects /Seamless Flow - Management and Security
    /Resources /Standards
      /RFC2119 - Indicating requirement levels
```

4.1.7. SF-MS-TERM1 – Digital Records Terminology

Terminology relating to digital records is defined in [**SF-MS-TERM1**]. It can be found in the National Archives file plan at:

```
/Information and Communication Technology
  /Projects /Seamless Flow - Management and Security
    /Deliverables
      /Digital Records Terminology SF-MS-TERM1
```

4.1.8. Seamless Flow Programme Glossary

The Seamless Flow programme glossary [**SF-GLOSSARY**] provides definitions of terminology across the Seamless Flow programme. It can be found in the National Archives file plan at:

```
/Strategic Management
  /Projects /Seamless Flow Programme
    /Central Project Direction
      /Glossary
```

4.1.9. Clark Wilson - a comparison of commercial and military security policies

This important paper in computer security outlines a security model for integrity protection based around the separation of duties and well-formed transactions [**CLARKWILSON**].

It differs from previous military models, which are mostly concerned with confidentiality, in that it is focussed on protecting internal and external integrity. It is not an entirely formalised model; instead it gives business rules for access designed to:

1. Prevent unauthorized users from making modifications to data or programs.
2. Prevent authorized users from making improper or unauthorized modifications.
3. Maintain internal and external consistency of data and programs.

This is achieved largely through the application of two principles:

- Separation of duties
- Well-formed transactions

It can be found on the Internet at:

http://crypto.stanford.edu/~ninghui/courses/Fall03/papers/clark_wilson.pdf

Or alternatively in Objective at:

```
/Information and Communication Technology
  /Projects /Seamless Flow - Management and Security
    /Resources /Standards
      /clark wilson integrity security model
```

4.1.10. Bell LaPadula – Secure Computer System: unified exposition

This seminal paper in computer security presents a formal model for protecting confidentiality in military or government applications [**BLP76**]. This is largely achieved through the comparison of security levels, although mathematically extended to accommodate more policy variations (such as need-to-know) by adding sets of labels to subjects and objects, not merely a single hierarchical level.

It can be found on the Internet at:

<http://csrc.nist.gov/publications/history/bell76.pdf>

Or alternatively in Objective at:

```
/Information and Communication Technology
  /Projects /Seamless Flow - Management and Security
    /Resources /Standards
      /Bell LaPadula - Secure Computer System
```

4.2. Document Glossary

The document glossary provides definitions of terms introduced in this document.

4.2.1. Access control terminology

access control decision	A yes/no decision given when a subject makes a request for access rights to an object .
access rights	The set of rights that a subject may request to an object .
detection	The detection of unauthorised access to an object .
closed material	Controlled objects that are not intended for public consumption by any method. This includes objects subject to FOI exemptions, Restricted material and the unredacted versions of records subject to the Data Protection Act.
constrained data item	(CDI) The output from a transformation procedure after validating a unconstrained data item .
controlled object	An object that belongs to the set of objects to which this access control policy applies.
dominate	A security level is said to dominate another security level if the value of the former is considered to be greater than or equal to the latter.
editorial right	A right that allows the creation, modification or destruction of a controlled object .
editorial role	A role which is assigned an editorial right .
execute right	An access right allowing a subject to execute a transformation procedure .
execute role	A role which is assigned an execute right .
external integrity	The correspondence of data in a system with the wider world; that the contents accurately describe what they purport to.
integrity verification procedure	A function whose purpose is to verify the internal integrity of the constrained data items within a system.
internal integrity	The correspondence of data to other data within a system; that the data is logically consistent with respect to itself. For example, that all relation constraints in a database are satisfied.
fully open material	open material for which there exists no explicit read access restrictions.

object	The passive entity involved in an access control decision ; the thing to which a subject requests access rights .
open material	Controlled objects that are intended to be publicly available to read by some method. This includes copyright and sensitive material, which while not published directly on the public Internet is still intended for public consumption by alternate means.
partially open material	open material for which there exists some explicit read access restrictions. An example may be sensitive material, not available on the Internet, but available through a reading room.
protective marking	A label attached to an object indicating its security classification .
permissions right	A right which permits a subject to change access rights on roles or to allocate roles to subjects.
permissions role	A role with a permissions right . A role with a permissions right must not have an editorial right .
prevention	The prevention of unauthorised access to an object .
reaction	The response to unauthorised access to an object .
read right	An access right that allows an information flow from an object to a subject .
restriction right	An editorial right that permits the security level of a controlled object to change.
restriction role	An editorial role with a restriction right .
right	A permission to access an object in various ways.
security classification	A hierarchical UK government record security classification which can be either Unclassified, Restricted, Confidential, Secret or Top Secret.
security labels	Labels attached to an object to restrict access. Only subjects possessing all the labels that an object possesses can access the object.
security level	A combination of a protective marking with a set of security labels .
strong authentication	A proof that a user is whom they claim to be, without the proving secret being revealed during the process.
subject	The active entity in an access control decision , the requestor of access rights to an object . A subject may be a user, or it may be a process running on a computer.
transformation procedure	The term given to a function or application which may create, modify, or delete a controlled object . The term comes from the seminal integrity model proposed in the Clark Wilson paper.

unconstrained data item	(UDI) The input to a transformation procedure before it is validated and entered into the system as a constrained data item .
user	A subject representing a human being or a process in the system.
write right	An access right that allows an information flow from a subject to an object .

5. Annex B

5.1. Protective markings

The UK government defines 4 hierarchical security classifications for the **protective marking** of records:

- Top secret
- Secret
- Confidential
- Restricted

If a record has no requirement for protective marking, it is called Unclassified.

The National Archives shall only deal with Unclassified or Restricted records at this time.

5.1.1. Unclassified records

Unclassified records have no general access restrictions, although access to various groups¹⁶, including the public, may still be limited by other considerations including FOI exemptions, sensitivity, copyright and data protection issues.

5.1.2. Restricted records

Restricted records must not have any public access¹⁷. Access to other groups¹⁸ may be further limited by other considerations, including originating department and conformance with government accreditation requirements to manage Restricted records.

Restricted records do not require specific security clearance in order to grant access to them, although a need-to-know principle should be applied, and a Basic Check (BC) clearance is recommended¹⁹.

¹⁶ These groups and their specific access restrictions will be formally defined in the Access Control Model document.

¹⁷ Unless suitably redacted, in which case the redacted record becomes a new record with its own appropriate security level.

¹⁸ These groups and their specific access restrictions will be formally defined in the Access Control Model document.

¹⁹ In some cases a CTC (Counter Terrorist Check) may be required to access Restricted records, but only where there is a demonstrable terrorist threat to the individual or the information is likely to be of value to terrorists. For precise details, consult the [MPS] or seek advice from the Departmental Security Officer.

5.2. Security levels

Where access control must be finer-grained than protective markings allow, this may be achieved by the use of additional **security labels**, which are assigned to each object and subject. The combination of a **protective marking** with a set of security labels shall be termed a **security level**.

5.2.1. Visualising security levels

It is useful to visualise security levels through an arrangement called a lattice²⁰.

For example, if we define security levels consisting of the protective markings “Unclassified” and “Restricted” with a set of two security labels {COPYRIGHT, SENSITIVE}, we can make a lattice with all the unique combinations of marking and label²¹.

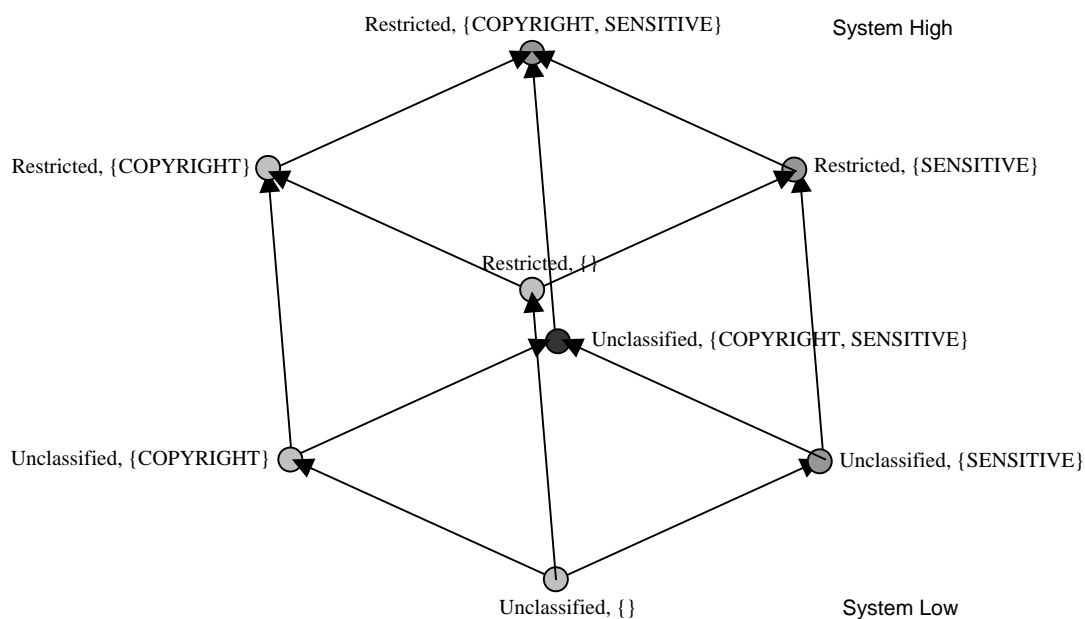


Figure 1 - a diagram of a lattice of security levels

Each node in the diagram²² represents a security level, a unique combination of a protective marking and a set of security labels. Each is connected to those neighbour nodes that have either a greater protective marking, or one additional label.

²⁰ A lattice is basically an arrangement of connected nodes where any two nodes always have a common node somewhere below them (if not already at the bottom), and a common node somewhere above them (if not already at the top).

²¹ Note that it is possible to have no labels at all. This is denoted by the empty set {}.

²² This diagram looks like a 3-D box, rather like the famous Necker Cube optical illusion. With more security labels, the number and combination of nodes increases, and it is no longer possible to make quite such a neat diagram.

5.2.2. Comparing security levels

For many nodes in the lattice, it is easy to see whether the security level of the node is greater or smaller than another node. For example, “*Restricted, {COPYRIGHT}*” is clearly a higher security level than “*Unclassified, {COPYRIGHT}*”. The greater node has equivalent or greater protective marking, and its labels at a minimum contain all the labels of the lower node.

If two levels are comparable in this way²³, a subject will be granted access to an object if the level of the subject is greater than or equal to the level of the object.

However, there are a few pairs of nodes for which this comparison does not work. For example, is “*Restricted, {}*” greater or smaller than “*Unclassified, {COPYRIGHT, SENSITIVE}*”? *Restricted* is greater than *Unclassified*, but *{}* is smaller than *{COPYRIGHT, SENSITIVE}*. They clearly represent different levels of access, but they are not meaningfully greater or smaller than each other.

If the levels are not comparable, a subject is not granted access to the object.

However, in order to implement this kind of access control, we do not have to construct a complex diagram and follow the arrows – this is only done in order to aid visualisation. There is a simpler method of achieving the same access control decisions. A subject is granted access to the object if:

1. The classification of the object is less than or equal to that of the subject.
2. All the labels in the object are also in the labels of the subject.

More formally, a subject *S* and an object *O* each have a security level *L*, denoted by L_S and L_O respectively. A security level *L* is a compound value composed of a classification *C*, and a set of security labels *X*, $L = (C, X)$.

S is granted access to *O* if $L_O \leq L_S$.

The operation \leq on the two security levels is defined as:

1. $C_O \leq C_S$
2. $X_O I X_S$

where *I* means that all the elements in the set on the left hand side are to be found on the right hand side.

²³ Security levels are only comparable in this way if it is possible to follow the arrows on the diagram in one direction only from one level to the other level.

5.2.3. Access control examples

For example, if we define three users with the following levels and roles:

U ₁	<i>Unclassified</i> , {}	a public user on the Internet.
U ₂	<i>Unclassified</i> , { <i>COPYRIGHT</i> }	a reader at Kew.
U ₃	<i>Restricted</i> , { <i>COPYRIGHT</i> , <i>SENSITIVE</i> , <i>FOI</i> }	a technology watch migration process.

And there are two records:

R ₁	<i>Unclassified</i> , { <i>COPYRIGHT</i> }	a record with copyright issues.
R ₂	<i>Unclassified</i> , { <i>COPYRIGHT</i> , <i>SENSITIVE</i> }	a sensitive record with copyright issues.

Then the following access control decisions would be made:

- U₁ cannot access R₁ or R₂, as he does not possess the *COPYRIGHT* security label.
- U₂ can access R₁, as the security levels are equivalent, but cannot access R₂, as she does not possess the *SENSITIVE* label.
- U₃ can access R₁ and R₂, as *Restricted* is higher than *Unclassified*, and it has all the labels in both records.

Adding labels to subjects and objects can easily extend this access control methodology. For example, limiting government departments to only those records with their own departmental label.