|  |
| --- |
| **Implementation Guidance**  **(this section must be removed from final version of the document)** |
| **Purpose of this document**  This procedure sets out how logs will be set up and managed in order to monitor system usage. |
| **Areas of the standard addressed**  The following areas of the ISO/IEC 27001:2013 standard are addressed by this document:  Annex A  A.12 Operations security  A.12.4 Logging and monitoring |
| **General Guidance**  The standard is fairly specific about what needs to be done in this area, including the need to log system administrator and system operator activities. You may need to look at various technical issues around this to try to ensure a consistent policy can be implemented effectively.  Third party software tools may help in meeting these requirements and in reducing the amount of administrative overhead involved. |
| **Review Frequency**  We would recommend that this document is reviewed annually and upon significant change to IT service provision. |
| **Toolkit Version Number**  ISO/IEC 27001 Toolkit Version 6 ©CertiKit 2015. |
| **Document Fields**  This document may contain fields which need to be updated with your own information, including a field for Organization Name that is linked to the custom document property “Organization Name”.  To update this field (and any others that may exists in this document):   1. Update the custom document property “Organization Name” by clicking File > Info > Properties > Advanced Properties > Custom > Organization Name 2. Press Ctrl a on the keyboard to select all text in the document (or use Select, Select All on the ribbon) 3. Press F9 on the keyboard to update all fields 4. When prompted, choose the option to just update TOC page numbers   If you wish to permanently convert the fields in this document to text i.e. so that they are no longer updateable, then you will need to click into each occurrence of the field and press Ctrl Shift F9.  If you would like to make all fields in the document visible then go to File > Options > Advanced > Show document content > Field shading and set this to “Always”. This can be useful to check that you have updated all fields correctly.  Further detail on the above procedure can be found in the *Toolkit Completion Instructions* within the Project Resources folder. |
| **Copyright notice**  Except for any third party works included in this document, as identified in this document, this document has been authored by CertiKit, and is © copyright CertiKit except as stated below.  CertiKit is a trading name of Public I.T. Limited, a company registered in England and Wales with company number 6432088 and registered office at 5 Falcons Rise, Belper, Derbyshire, DE56 0QN. |
| **Licence terms**  This document is licensed on and subject to the standard licence terms of CertiKit, available on request, or by download from our website. All other rights are reserved. Unless you have purchased this product you only have an evaluation licence. If this product was purchased, a full licence is granted to the person identified as the licensee in the relevant purchase order. The standard licence terms include special terms relating to any third party copyright included in this document. |
| **Disclaimer**  **Please Note:** *Your use of and reliance on this document template is at your sole risk. Document templates are intended to be used as a starting point only from which you will create your own document and to which you will apply all reasonable quality checks before use. Therefore please note that it is your responsibility to ensure that the content of any document you create that is based on our templates is correct and appropriate for your needs and complies with relevant laws in your country. You should take all reasonable and proper legal and other professional advice before using this document. CertiKit makes no claims, promises, or guarantees about the accuracy, completeness, or adequacy of our document templates, assumes no duty of care to any person with respect its document templates or their contents, and expressly excludes and disclaims liability for any cost, expense, loss or damage suffered or incurred in reliance on our document templates, or in expectation of our document templates meeting your needs, including (without limitation) as a result of misstatements, errors and omissions in their contents.* |

**E:\valuementor-policies\pics\vm-logo-small.jpg**

**Procedure for Monitoring**

**Use of IT Systems**

|  |  |
| --- | --- |
| **Document Classification:** |  |
| **Document Ref.** | **ISMS18002** |
| **Version:** | **1** |
| **Dated:** | **Insert date** |
| **Document Author:** |  |
| **Document Owner:** |  |

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Revision Author** | **Summary of Changes** |
|  |  |  |  |
|  |  |  |  |

**Distribution**

|  |  |
| --- | --- |
| **Name** | **Title** |
|  |  |
|  |  |
|  |  |

**Approval**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Position** | **Signature** | **Date** |
|  |  |  |  |

**Contents**

[1 Introduction 7](#_Toc414090349)

[1.1 Risks Addressed 7](#_Toc414090350)

[1.2 Scope 7](#_Toc414090351)

[1.3 Related Documents 7](#_Toc414090352)

[1.4 Purpose 7](#_Toc414090353)

[2 Procedure 8](#_Toc414090354)

[2.1 Audit Logging 8](#_Toc414090355)

[2.2 Monitoring System Use 10](#_Toc414090356)

[2.3 Protection of Log Information 10](#_Toc414090357)

[2.4 Administrator and Operator Logs 10](#_Toc414090358)

[2.5 Fault Logging 11](#_Toc414090359)

[2.6 Clock Synchronisation 11](#_Toc414090360)

# Introduction

## Risks Addressed

This document describes a control that was identified in ISMS06004 Information Security Risk Treatment Plan to address the following risks:

|  |  |
| --- | --- |
| **Reference** | **Description of Risk** |
| [Reference] | [List the identified risks to which this control is intended to apply] |
|  |  |
|  |  |

## Scope

This control applies to all systems, people and processes that constitute the organization’s information systems, including board members, directors, employees, suppliers and other third parties who have access to [Organization Name]systems.

## Related Documents

The following policies and procedures are relevant to this document:

* ISMS14002 Information Security Classification Guidelines
* ISMS13001 AUP and Personal Commitment Statement
* ISMS13002 Email Policy
* ISMS13003 Internet Acceptable Use Policy

## Purpose

In order to ensure that [Organization Name]information assets are kept secure at all times, it is necessary to monitor the activities of both authorised and unauthorised users to identify any actions that are not in keeping with the secure use of the facilities provided. Such actions may include:

* Unauthorised access attempts
* Unusual use of privileged accounts e.g. administrator
* Attachment of unauthorised removable media devices
* Unusual patterns of activity e.g. late at night
* Changes to system settings

This procedure sets out the ways in which such monitoring is carried out. It should be read in conjunction with document ISMS22001Information Security Incident Management Procedure which sets out what actions are taken in the event that an actual or potential security is detected.

# Procedure

## Audit Logging

All clients, servers and other equipment (such as network routers and switches) involved in hosting the storage or processing of classified information will have the available audit logging facilities activated. This allows us to record and monitor activities in the following areas:

* Dates and times of key events e.g. log on/log off
* Successful and rejected systems access attempts
* Successful and rejected data and other resource access attempts
* Changes to system parameters and configurations
* Use of system utilities and applications

This information gives us a picture of what is happening on individual devices such as servers and, where available, within individual applications.

The general principle adopted is that the higher the level of classification of the information held or processed, the greater the level of detail the audit logs will record data to.

The table below summarises the level of logging that is in place on each type of device for each classification of information being processed within .

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Information Classification** | **Level of Audit Logging** | | | | | |
| **Clients** | **Windows servers** | **UNIX servers** | **Cisco Routers** | **Firewalls** | **Switches** |
| Public | [define the audit settings in place] | [define the audit settings in place] | [define the audit settings in place] | [define the audit settings in place] | [define the audit settings in place] | [define the audit settings in place] |
| Protected | [define the audit settings in place] | [define the audit settings in place] | [define the audit settings in place] | [define the audit settings in place] | [define the audit settings in place] | [  define the audit settings in place] |
| Restricted | [define the audit settings in place] | [define the audit settings in place] | [define the audit settings in place] | [define the audit settings in place] | [define the audit settings in place] | [define the audit settings in place] |
| Confidential | [define the audit settings in place] | [define the audit settings in place] | [define the audit settings in place] | [define the audit settings in place] | [define the audit settings in place] | [define the audit settings in place] |

*Figure 1 – Audit setting by type of device*

## Monitoring System Use

The contents of audit logs will be reviewed on a regular basis according to the:

* business criticality of the application
* classification of the information assets involved
* frequency with which systems have been attacked or compromised previously
* level of exposure to external networks

It is impossible to manually review all audited events within all audit logs so it is important that the most critical systems are addressed first and that log events are filtered as much as possible.

Where possible, log management software will be used to identify events worth immediate investigation and to find potential links between events on multiple systems.

The following events will be investigated as a matter of urgency:

* Unauthorised removable device attachment
* Unauthorised download of sensitive information
* Changes to systems security settings and controls
* Alerts from intrusion detection systems
* Unusual use of privileged accounts e.g. administrator
* [add further events as relevant to your organization]

Investigation will be carried out according to the procedures set out in document ISMS22001Information Security Incident Management Procedure.

## Protection of Log Information

Log files will be kept for a period of six months. Strict permissions will be used to ensure that the contents of log files cannot be altered after they have been written. Where possible, key events from log files will be copied to a central point and archived. Backups of log files will be taken on a daily basis.

## Administrator and Operator Logs

Logs will be taken of all administrator and operator activities so that it is possible to identify the actions that were carried out under such user accounts. Whilst this may not be necessary for every system within , those holding Restricted and Confidential classification information or involving a financial element should be monitored more closely.

See document ISMS14001 Information Asset Inventory for more details.

## Fault Logging

Error logging will be enabled on all systems and applications dealing with classified information and all reported faults will be investigated to ensure that security controls have not been compromised.

Faults should in the first instance be logged via the IT Service Desk and will be investigated according to the organization’s standard incident management process.

## Clock Synchronisation

Where possible, all systems should synchronise their date and time either with a single internal source or an appropriate external time source. This is important so that events on different systems can be correctly compared without having to consider differences in system times.

Within [Organization Name]the following convention will be used:

* All client desktop computers and member servers will synchronise with their domain controller
* All domain controllers in a domain will synchronise with the primary domain controller (PDC) operations master
* All PDC operations masters follow the hierarchy of domains in their time synchronisation

[Describe how time synchronisation will be achieved]