

<< [Organisation] Logo>>

<< System Configuration Policy >>

Version: 1.0

Date

Version: xx

Date: xx

[Organisation] Name: xx

Security Level: Internal

Page 1 of 5

NetHost Legislation- Cyber Essentials and ISO Standard Management System Certification, Scotland/England

info@nethostlegislation.co.uk,

www.nethostlegislation.co.uk

Revision History

Date	Version	Author	Summary of Changes

Approvals

Name	Signature	Title	Issue Date	Version

Version: xx

Date: xx

[Organisation] Name: xx

Security Level: Internal

Page 2 of 5

NetHost Legislation- Cyber Essentials and ISO Standard Management System Certification, Scotland/England

info@nethostlegislation.co.uk,www.nethostlegislation.co.uk

Contents

Contents

INTRODUCTION	4
DOCUMENT PURPOSE.....	4
SCOPE	4
POLICY	4

Version: xx

Date: xx

[Organisation] Name: xx

Security Level: Internal

Page 3 of 5

NetHost Legislation- Cyber Essentials and ISO Standard Management System Certification, Scotland/England

info@nethostlegislation.co.uk,

www.nethostlegislation.co.uk

INTRODUCTION

DOCUMENT PURPOSE

This policy document sets forth best practice system configuration setting to ensure integrity, confidentiality and availability of data stores/process/transmitted in the systems.

SCOPE

All system components within, or connected, to the [organisation]'s are within scope of these procedures.

POLICY

Below are statements that should be complied with: -

Policy Statements

No:	Statements
	Prior to installing a system on the network, all vendor-supplied defaults (including but not limited to passwords, simple network management protocol (SNMP), and community strings) are changed and unnecessary accounts eliminated.

Version: xx

Date: xx

[Organisation] Name: xx

Security Level: Internal

Page 4 of 5

NetHost Legislation- Cyber Essentials and ISO Standard Management System Certification, Scotland/England

info@nethostlegislation.co.uk,

www.nethostlegislation.co.uk

SYSTEM CONFIGURATION POLICY

	International best practice hardening standards should be used to benchmark [organisation] system configuration. Industry-accepted hardening standards e.g. SANS, NIST & CIS.
	System configuration standards are applied whenever new systems are configured.
	All unnecessary and insecure services, protocols & daemons are disabled, or if required for business purposes, are justified and documented as to the appropriate use of the service within the specific configuration standard and appropriate security features (technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP) have been identified, documented and implemented.
	All unnecessary functionality, including scripts, drivers, features, subsystems, file systems, and unnecessary web servers are removed from system components.
	All high-risk or critical security updates for operating systems, applications and firmware are installed within 14 days of release

Version: xx

Date: xx

[Organisation] Name: xx

Security Level: Internal

Page 5 of 5

NetHost Legislation- Cyber Essentials and ISO Standard Management System Certification, Scotland/England

info@nethostlegislation.co.uk,

www.nethostlegislation.co.uk