

# **NT4 Generic Security Standard**

---

# NT4 Generic Security Standard

Published 16 May 2009

Copyright © 2001, 2002, 2003, 2009 Frank O'Dwyer

This document specifies generic technical security policy for implementations of Microsoft Windows NT4.0, and applies to workstation, server and domain controller implementations of NT4.0, whether standalone or part of a domain.

This standard contains 36 baseline controls, and 3 above baseline controls, for a total of 39 controls.

## **Important**

All of these Security Standards and Security Policies are copyrighted. **THEY ARE NOT IN THE PUBLIC DOMAIN.** They are however distributed under a liberal open-source license, see Publishing these Security Standards and Policies.

---

---

---

# Table of Contents

1. Introduction .....	1
1.1. Objectives .....	1
1.2. Scope .....	1
1.3. Not In Scope .....	1
1.4. Giving Feedback .....	1
1.5. Publishing these Security Standards and Policies .....	1
1.6. Related Documents .....	2
1.6.1. Generic Security Standards .....	2
1.6.2. Operating System Security Standards .....	3
1.6.3. Database Security Standards .....	3
1.7. Definitions .....	3
2. User Configuration .....	4
2.1. User Administration .....	4
2.1.1. Restrict access to login scripts and profiles .....	4
2.2. Default Accounts .....	4
2.2.1. Rename the administrator account .....	4
2.2.2. Disable Guest Account .....	5
2.3. Privileges .....	6
2.3.1. The advanced user right to load and unload device drivers must not be assigned to any users .....	6
2.3.2. The advanced user right to create a page file must not be assigned to any users .....	6
2.3.3. The advanced user right to bypass traverse checking must not be assigned to any users .....	7
2.3.4. The advanced user right to profile single process must be assigned only to administrators. ....	8
2.3.5. The advanced user right to replace a system level process token must be assigned to no user .....	8
2.3.6. The advanced user right to create permanent shared objects must not be assigned to any users .....	9
2.3.7. The advanced user right to generate security audits must not be assigned to any users other than administrators or security teams .....	10
2.3.8. The advanced user right to debug programs must be assigned only to administrators and developers .....	10
2.3.9. The user right to shutdown the system should be assigned to local groups and not to individual users .....	11
2.3.10. The advanced user right to profile system performance must be assigned only to administrators. ....	12
2.3.11. The advanced user right to receive unsolicited device input must be assigned to no users. ....	12
2.3.12. The user right to force shutdown from a remote system should be assigned to local groups and not to individual users .....	13
2.3.13. The advanced user right to increase scheduling priority must be assigned only to administrators .....	14
2.3.14. The advanced user right to modify firmware environment variables must only be assigned to administrators. ....	14
2.3.15. The advanced user right to act as part of the operating system must be assigned to no one. ....	15
2.3.16. The advanced user right to create a token object must not be assigned to any users .....	16
2.3.17. The user right to logon locally should be assigned to local groups and not to individual users .....	16
2.3.18. The user right to change the system time should be assigned to local groups .....	16

and not to individual user .....	17
2.3.19. The advanced user right to logon as a service must be assigned only to administrators .....	18
3. Security Compliance .....	19
3.1. Security Management .....	19
3.1.1. Antivirus software must be installed and maintained current on all machines	19
3.1.2. Ensure that a legal notice appropriate to your jurisdiction is displayed in the legal notice placeholder for display prior to logon .....	19
4. Network Security Configuration .....	21
4.1. Network Interface Considerations .....	21
4.1.1. FTP should not be installed or if part of the default image it should be disabled .....	21
5. Configuration .....	22
5.1. Files and File Permissions .....	22
5.1.1. Use encryption for sensitive data files .....	22
5.2. Administration .....	22
5.2.1. Clear Page File at Shutdown .....	22
6. Installation .....	24
6.1. Setup Choices .....	24
6.1.1. Do not use dual-boot .....	24
6.1.2. Restrict access to alternate boot mechanisms .....	24
6.1.3. Delete \$WinNT\$.inf files .....	25
6.1.4. Installation disk image duplication .....	25
6.1.5. Format all disk partitions with NTFS .....	26
6.1.6. Do not use HPFS or FAT file structures. Always use NTFS. ....	27
7. Auditing and Monitoring .....	28
7.1. Audit log destination and format .....	28
7.1.1. Security event logging must be enabled and not set to overwrite events .....	28
7.2. Events to be audited .....	28
7.2.1. Set up file auditing for group everyone .....	28
7.2.2. Set up directory auditing for group everyone .....	29
7.2.3. Network alerts must be enabled for excessive login failures .....	30
7.2.4. The audit policy must be set up to record failure and success for Logon and Logoff, User and Group Management, Security Policy Changes, Restart, Shutdown and System and failure for File and Object Access .....	31
7.2.5. Set up registry key auditing for group everyone .....	32
8. Checklist .....	34

---

---

---

# Chapter 1. Introduction

## 1.1. Objectives

The objectives of this document are:

- To specify a baseline configuration for implementations of <trademark>Microsoft</trademark> <trademark>Windows</trademark> NT4.0.
- To provide guidance to administrators, developers and security personnel in securely implementing <trademark>Microsoft</trademark> <trademark>Windows</trademark> NT4.0.

## 1.2. Scope

Controls specified in this document apply to workstation, server, and domain controller implementations of NT4.0, whether used standalone or part of a domain.

All of the organisation's NT4.0 information systems will be subject to the policies specified within this generic security standard. The policies will be applied to new and existing installations.

## 1.3. Not In Scope

Compliance with this standard will not provide “in depth” security architecture or intelligent security design guidance to projects. As a consequence, for high impact or safety-critical business applications, additional guidance will still need to be sought from the Information Security team consultancy function.

This is a generic standard. Controls specific to workstation, server, or domain controller implementations are not defined here but will be the subject of additional standards.

Compliance with this standard does not negate the need for an overall security review of a proposed application. Contact the Information Security team if you are in doubt.

## 1.4. Giving Feedback

Your feedback to improve this document is welcome. Please let me know of your experiences in applying the controls and guidance in this standard. Are the controls effective, easy to implement, too onerous, clear, unclear, something missing? Does an exceptional case need to be covered? Let me know. Please send your comments to frankodwyer AT netscape.net. Your comments will be used to produce better free security standards for the IT community.

I also request that you give feedback where you think the controls and guidance is correct. This will let us gauge whether or not specific controls are controversial or broadly acceptable to the community, and will help us to resolve cases where we have conflicting feedback on particular content.

## 1.5. Publishing these Security Standards and Policies

This document may be reproduced and distributed in whole or in part, free of charge, subject to the fol-

following conditions:

- All copyright and trademark notices, and this permission notice must be preserved complete on all complete or partial copies.
- Any translation or derivative work of this document must be approved by Frank O'Dwyer in writing before distribution.
- If you distribute this guide in part, instructions for obtaining the complete version of this manual must be included, and a means for obtaining a complete version provided.
- Small portions may be reproduced as illustrations for reviews or quotes in other works without this permission notice if proper citation is given.
- Neither Frank O'Dwyer's name nor the names of any contributors may be used to endorse or promote products derived from this document without specific prior written permission.

THIS DOCUMENT IS PROVIDED BY FRANK O'DWYER AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL FRANK O'DWYER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

I would like to be informed of any plans to publish or distribute these documents, just so I know how they're being used and where they are becoming available. If you are publishing or distributing or planning to publish or distribute any of these documents, please send mail to frankodwyer AT netscape.net

## 1.6. Related Documents

This document should be read and applied in conjunction with the technology specific security standards that are available from the frankodwyer.com web site. Please note that some of the documents below are currently under development and as such may not as yet be available. Check back frequently for updates to this document and those documents listed below.

### 1.6.1. Generic Security Standards

*Generic Security Standards*

<http://www.frankodwyer.com/standards/index.html#generic>

*Data Protection European Union Security Standard*

<http://www.frankodwyer.com/standards/index.html#generic>

*Application Service Provider Security Standards*

<http://www.frankodwyer.com/standards/index.html#generic>

## 1.6.2. Operating System Security Standards

*Generic Unix Security Standards*

<http://www.frankodwyer.com/standards/index.html#os>

*Windows NT4.0 Generic Security Standards*

<http://www.frankodwyer.com/standards/index.html#os>

*Windows NT4.0 Workstation Security Standards*

<http://www.frankodwyer.com/standards/index.html#os>

*Windows NT4.0 Server Security Standards*

<http://www.frankodwyer.com/standards/index.html#os>

*Windows NT4.0 Domain Security Standards*

<http://www.frankodwyer.com/standards/index.html#os>

## 1.6.3. Database Security Standards

*Oracle Security Standards*

<http://www.frankodwyer.com/standards/index.html#db>

## 1.7. Definitions

An “Information Asset” equates to any computerised information system or component thereof and thus includes an application, an item of off the shelf software, hardware, media, a data item, a data item repository and associated communications networks.

The specification of the Information Asset in question will usually be given so that this document is unambiguous, except where a control relates to any “Information Asset”.

The use of “must” or “will” indicates what the author considers to be a mandatory control.

However, whether the controls listed here are mandatory for your organisation is entirely at your organisation's discretion and thus they should be interpreted as representing the strongest recommendation of the author.

The use of “should” or “recommended” or “ought” indicates that the author believes that the controls in question are worthwhile and should be implemented unless such an implementation is impossible, onerous or impractical. Again, the implementation of controls so recommended in this document is entirely at your organisation's discretion.

---

# Chapter 2. User Configuration

## 2.1. User Administration

### 2.1.1. Restrict access to login scripts and profiles

ID	Version	Level	Enforcement
NT4GEN-UC-1	1.0	baseline	mandatory

#### 2.1.1.1. Standard

Login scripts and profiles must be accessible only by their user and administrators.

#### 2.1.1.2. Detailed Steps

- Ensure the ACLs for login scripts and profiles grant access only to their user and administrators.

#### 2.1.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Users will be able to run programs using the privileges of other users.
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

## 2.2. Default Accounts

### 2.2.1. Rename the administrator account

ID	Version	Level	Enforcement
NT4GEN-DA-2	1.0	baseline	recommended

#### 2.2.1.1. Standard

Rename the administrator to an attributable account name and assign a new password.

#### 2.2.1.2. Detailed Steps

- Rename the administrator account to an individuals name
- Assign a new password

### 2.2.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- As the admin account is certain to exist on every system it is a priority for attack
- Changing the password from the default helps prevent unauthorised access
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

## 2.2.2. Disable Guest Account

ID	Version	Level	Enforcement
NT4GEN-DA-1	1.0	baseline	mandatory

### 2.2.2.1. Standard

The guest account must be disabled.

### 2.2.2.2. Detailed Steps

- Select account disabled on the main account window.
- Give the guest account a long random password that is not retained by anyone.
- Set its login hours to none.
- Set its expiration date to a date past.

### 2.2.2.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised network access to the NT system may be possible.
- Unauthorised access to NT objects may result
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.

- Business information and applications may be unavailable.

## 2.3. Privileges

### 2.3.1. The advanced user right to load and unload device drivers must not be assigned to any users

ID	Version	Level	Enforcement
NT4GEN-PRIV-13	1.0	baseline	mandatory

#### 2.3.1.1. Standard

The advanced user right to load and unload device drivers must not be assigned to any users

#### 2.3.1.2. Detailed Steps

- Identify all users who hold this right and revoke it.
- Identify all applications who hold this right and determine why they need it and revoke it for all those where this requirement is clearly spurious

#### 2.3.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Replacing a device driver may be used to gain unauthorised access
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

### 2.3.2. The advanced user right to create a page file must not be assigned to any users

ID	Version	Level	Enforcement
NT4GEN-PRIV-7	1.0	baseline	mandatory

#### 2.3.2.1. Standard

The advanced user right to create a page file must not be assigned to any users

### 2.3.2.2. Detailed Steps

- Identify all users who hold this right and revoke it.
- Identify all applications who hold this right and determine why they need it and revoke it for all those where this requirement is clearly spurious

### 2.3.2.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

## 2.3.3. The advanced user right to bypass traverse checking must not be assigned to any users

ID	Version	Level	Enforcement
NT4GEN-PRIV-6	1.0	baseline	mandatory

### 2.3.3.1. Standard

The advanced user right to bypass traverse checking must not be assigned to any users

### 2.3.3.2. Detailed Steps

- Identify all users who hold this right and revoke it.
- Identify all applications who hold this right and determine why they need it and revoke it for all those where this requirement is clearly spurious

### 2.3.3.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- This right permits access control on an object path to be disregarded and may result in unintended access being obtained
- Business information may be accidentally or maliciously altered.

- Business information may be disclosed.
- Business information and applications may be unavailable.

### 2.3.4. The advanced user right to profile single process must be assigned only to administrators.

ID	Version	Level	Enforcement
NT4GEN-PRIV-16	1.0	baseline	mandatory

#### 2.3.4.1. Standard

The advanced user right to profile single process must be assigned only to administrators

#### 2.3.4.2. Detailed Steps

- Identify all users who hold this right and revoke it.
- Identify all applications who hold this right and determine why they need it and revoke it for all those where this requirement is clearly spurious

#### 2.3.4.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- The ability to profile single processes may result in unauthorised disclosure of security sensitive information
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

### 2.3.5. The advanced user right to repace a system level process token must be assigned to no user

ID	Version	Level	Enforcement
NT4GEN-PRIV-19	1.0	baseline	mandatory

#### 2.3.5.1. Standard

The advanced user right to replace a system level process token must be assigned to no user

### 2.3.5.2. Detailed Steps

- Identify all users who hold this right and revoke it.
- Identify all applications who hold this right and determine why they need it and revoke it for all those where this requirement is clearly spurious

### 2.3.5.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Such access may be used to subvert the security controls on the system
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

## 2.3.6. The advanced user right to create permanent shared objects must not be assigned to any users

ID	Version	Level	Enforcement
NT4GEN-PRIV-9	1.0	baseline	mandatory

### 2.3.6.1. Standard

The advanced user right to create permanent shared objects must not be assigned to any users

### 2.3.6.2. Detailed Steps

- Identify all users who hold this right and revoke it.
- Identify all applications who hold this right and determine why they need it and revoke it for all those where this requirement is clearly spurious

### 2.3.6.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.

- Business information and applications may be unavailable.

### **2.3.7. The advanced user right to generate security audits must not be assigned to any users other than administrators or security teams**

<b>ID</b>	<b>Version</b>	<b>Level</b>	<b>Enforcement</b>
NT4GEN-PRIV-11	1.0	baseline	mandatory

#### **2.3.7.1. Standard**

The advanced user right to generate security audits must not be assigned to any users other than administrators or security teams

#### **2.3.7.2. Detailed Steps**

- Identify all users who hold this right and revoke it where appropriate
- Identify all applications who hold this right and determine why they need it and revoke it for all those where this requirement is clearly spurious

#### **2.3.7.3. Risks Addressed**

Where this control is not applied, the following residual risks exist:

- The security audit will contain disclosure sensitive information
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

### **2.3.8. The advanced user right to debug programs must be assigned only to administrators and developers**

<b>ID</b>	<b>Version</b>	<b>Level</b>	<b>Enforcement</b>
NT4GEN-PRIV-10	1.0	baseline	mandatory

#### **2.3.8.1. Standard**

The advanced user right to debug programs must be assigned only to administrators and developers

---

### 2.3.8.2. Detailed Steps

- Identify all users who hold this right and revoke it.
- Identify all applications who hold this right and determine why they need it and revoke it for all those where this requirement is clearly spurious

### 2.3.8.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Security sensitive information may be obtained such as passwords
- Unauthorised access may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

## 2.3.9. The user right to shutdown the system should be assigned to local groups and not to individual users

ID	Version	Level	Enforcement
NT4GEN-PRIV-4	1.0	baseline	recommended

### 2.3.9.1. Standard

The user right to shutdown the system should be assigned to local groups and not to individual users

### 2.3.9.2. Detailed Steps

- Assign the right to a local group
- Assign users to the group

### 2.3.9.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Administration should be performed using roles supported through membership of groups
- Complex individual admin often leads to unauthorised access
- Business information may be accidentally or maliciously altered.

- Business information may be disclosed.
- Business information and applications may be unavailable.

### **2.3.10. The advanced user right to profile system performance must be assigned only to administrators.**

<b>ID</b>	<b>Version</b>	<b>Level</b>	<b>Enforcement</b>
NT4GEN-PRIV-17	1.0	baseline	mandatory

#### **2.3.10.1. Standard**

The advanced user right to profile system performance must be assigned only to administrators.

#### **2.3.10.2. Detailed Steps**

- Identify all users who hold this right and revoke it.
- Identify all applications who hold this right and determine why they need it and revoke it for all those where this requirement is clearly spurious

#### **2.3.10.3. Risks Addressed**

Where this control is not applied, the following residual risks exist:

- The ability to profile system performance may result in a denial of service
- Business information and applications may be unavailable.

### **2.3.11. The advanced user right to receive unsolicited device input must be assigned to no users.**

<b>ID</b>	<b>Version</b>	<b>Level</b>	<b>Enforcement</b>
NT4GEN-PRIV-18	1.0	baseline	mandatory

#### **2.3.11.1. Standard**

The advanced user right to receive unsolicited device input must be assigned to no users.

#### **2.3.11.2. Detailed Steps**

- Identify all users who hold this right and revoke it.
- Identify all applications who hold this right and determine why they need it and revoke it for all those where this requirement is clearly spurious

### 2.3.11.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- This right can be used to obtain unauthorised access
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

## 2.3.12. The user right to force shutdown from a remote system should be assigned to local groups and not to individual users

ID	Version	Level	Enforcement
NT4GEN-PRIV-2	1.0	baseline	recommended

### 2.3.12.1. Standard

The user right to force shutdown from a remote system should be assigned to local groups and not to individual users

### 2.3.12.2. Detailed Steps

- Assign the right to a local group
- Assign users to the group

### 2.3.12.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Security administration is simplified by the use of roles
- This privilege may allow a denial of service to be executed
- Business information and applications may be unavailable.

### 2.3.13. The advanced user right to increase scheduling priority must be assigned only to administrators

ID	Version	Level	Enforcement
NT4GEN-PRIV-12	1.0	baseline	mandatory

#### 2.3.13.1. Standard

The advanced user right to increase scheduling priority must be assigned only to administrators

#### 2.3.13.2. Detailed Steps

- Identify all users who hold this right and revoke it.
- Identify all applications who hold this right and determine why they need it and revoke it for all those where this requirement is clearly spurious

#### 2.3.13.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- The ability to increase scheduling priority can be used to hog system resource
- This privilege may allow an enterprise wide denial of service
- Business information and applications may be unavailable.

### 2.3.14. The advanced user right to modify firmware environment variables must only be assigned to administrators.

ID	Version	Level	Enforcement
NT4GEN-PRIV-15	1.0	baseline	mandatory

#### 2.3.14.1. Standard

The advanced user right to modify firmware environment variables must be assigned only to administrators.

#### 2.3.14.2. Detailed Steps

- Identify all users who hold this right and revoke it.

- Identify all applications who hold this right and determine why they need it and revoke it for all those where this requirement is clearly spurious

### 2.3.14.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Modification of such variables may result in abnormal or unauthorised function
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

### 2.3.15. The advanced user right to act as part of the operating system must be assigned to no one.

ID	Version	Level	Enforcement
NT4GEN-PRIV-5	1.0	baseline	mandatory

#### 2.3.15.1. Standard

The advanced user right to act as part of the operating system must be assigned to no one.

#### 2.3.15.2. Detailed Steps

- Identify all users who hold this right and revoke it.
- Identify all applications who hold this right and determine why they need it and revoke it for all those where this requirement is clearly spurious

#### 2.3.15.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Acting as part of the operating permits privileged action to be undertaken
- Privileged action may be used to subvert operating system controls
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

## 2.3.16. The advanced user right to create a token object must not be assigned to any users

ID	Version	Level	Enforcement
NT4GEN-PRIV-8	1.0	baseline	mandatory

### 2.3.16.1. Standard

The advanced user right to create a token object must not be assigned to any users

### 2.3.16.2. Detailed Steps

- Identify all users who hold this right and revoke it.
- Identify all applications who hold this right and determine why they need it and revoke it for all those where this requirement is clearly spurious

### 2.3.16.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- The ability to create a token object may undermine the authentication system
- Unauthorised access may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

## 2.3.17. The user right to logon locally should be assigned to local groups and not to individual users

ID	Version	Level	Enforcement
NT4GEN-PRIV-3	1.0	baseline	recommended

### 2.3.17.1. Standard

The user right to logon locally should be assigned to local groups and not to individual users.

### 2.3.17.2. Detailed Steps

- Assign the right to a local group
- Assign users to the group

### 2.3.17.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Managing access rights by role simplifies administration
- Complex administration often results in unauthorised access.
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

## 2.3.18. The user right to change the system time should be assigned to local groups and not to individual user

ID	Version	Level	Enforcement
NT4GEN-PRIV-1	1.0	baseline	recommended

### 2.3.18.1. Standard

The user right to change the system time should be assigned to local groups and not to individual users.

### 2.3.18.2. Detailed Steps

- Assign the right to a local group
- Assign users to the group

### 2.3.18.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Reconstructing a set of events requires confidence in time sequencing
- Certain elements of security infrastructure are sensitive to time
- Changing the system time may mask unauthorised activity
- Changing the system time may result in unauthorised access
- Business information may be accidentally or maliciously altered.

- Business information may be disclosed.
- Business information and applications may be unavailable.

## 2.3.19. The advanced user right to logon as a service must be assigned only to administrators

ID	Version	Level	Enforcement
NT4GEN-PRIV-14	1.0	baseline	mandatory

### 2.3.19.1. Standard

The advanced user right to logon as a service must be assigned only to administrators

### 2.3.19.2. Detailed Steps

- Identify all users who hold this right and revoke it.
- Identify all applications who hold this right and determine why they need it and revoke it for all those where this requirement is clearly spurious

### 2.3.19.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- The ability to create processes as a services can be used to subvert the security controls and gain unauthorised access
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

---

# Chapter 3. Security Compliance

## 3.1. Security Management

### 3.1.1. Antivirus software must be installed and maintained current on all machines

ID	Version	Level	Enforcement
NT4GEN-VIRUS-1	1.0	baseline	mandatory

#### 3.1.1.1. Standard

Ant-virus software must be installed and maintained on all machines.

#### 3.1.1.2. Detailed Steps

- Install anti-virus software on all machines.
- Ensure that the virus engine and signature data files are maintained up to date

#### 3.1.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Virus infections can often subvert system security controls
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

### 3.1.2. Ensure that a legal notice appropriate to your jurisdiction is displayed in the legal notice placeholded for display prior to logon

ID	Version	Level	Enforcement
NT4GEN-LEGAL-1	1.0	baseline	mandatory

#### 3.1.2.1. Standard

Ensure that a legal notice appropriate to your jurisdiction is displayed in the legal notice placeholder for display prior to logon

### **3.1.2.2. Detailed Steps**

- Determine the most appropriate legal notice to implement for your jurisdiction
- Populate the legal notice placeholder with this message for display prior to logon

### **3.1.2.3. Risks Addressed**

Where this control is not applied, the following residual risks exist:

- Legal action following a subjected breach may prove problematic
- Monitoring of authorised use may prove problematic
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

---

# Chapter 4. Network Security Configuration

## 4.1. Network Interface Considerations

### 4.1.1. FTP should not be installed or if part of the default image it should be disabled

ID	Version	Level	Enforcement
NT4GEN-NETW-1	1.0	above baseline	recommended

#### 4.1.1.1. Standard

FTP should not be installed or if part of the default image it should be disabled

#### 4.1.1.2. Detailed Steps

- Build a server, w/s or domain controller image that does not include ftp by default
- Alternatively, disable ftp on w/s, servers and controllers where not needed

#### 4.1.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

---

# Chapter 5. Configuration

## 5.1. Files and File Permissions

### 5.1.1. Use encryption for sensitive data files

ID	Version	Level	Enforcement
NT4GEN-FILE-1	1.0	above baseline	mandatory

#### 5.1.1.1. Standard

Sensitive data files must be encrypted.

#### 5.1.1.2. Detailed Steps

- Use an encryption tool or an encrypted file system to store sensitive data files.

#### 5.1.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Sensitive data files will be accessible using non-standard tools when the NT operating system does not have control.
- Sensitive data files which have been deleted may be accessible using non-standard tools when the NT operating system does not have control.
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

## 5.2. Administration

### 5.2.1. Clear Page File at Shutdown

ID	Version	Level	Enforcement
NT4GEN-ADM-1	1.0	baseline	mandatory

#### 5.2.1.1. Standard

Enable clearing of the system page file at shutdown.

### 5.2.1.2. Detailed Steps

- Set the registry key HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SessionManager\Memory Management\ClearPageFileAtShutdown to 1.

### 5.2.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Sensitive information, including local and remote passwords and business information, may remain in the pagefile after shutdown. This may be recoverable by an attacker who has physical access to the machine.
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

---

# Chapter 6. Installation

## 6.1. Setup Choices

### 6.1.1. Do not use dual-boot

ID	Version	Level	Enforcement
NT4GEN-SETUP-2	1.0	baseline	mandatory

#### 6.1.1.1. Standard

NT must be the only operating system installed. The system must not be set up to dual-boot other operating systems.

#### 6.1.1.2. Detailed Steps

- Remove other operating systems by formatting partitions to NTFS prior to installation.
- Ensure that boot.ini automatically boots NT, and that it lists no other operating systems.

#### 6.1.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Filesystems will not be protected by NT ACLs.
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

### 6.1.2. Restrict access to alternate boot mechanisms

ID	Version	Level	Enforcement
NT4GEN-SETUP-3	1.0	above baseline	mandatory

#### 6.1.2.1. Standard

Only authorised users must be able to boot the system from alternative media (CD, floppy disk).

#### 6.1.2.2. Detailed Steps

- Ensure that the BIOS boot order boots from the hard disk before CD, floppy, or other bootable devices.
- Assign a BIOS password to prevent changes to the boot order, and restrict access to the BIOS password to authorised personnel.

### 6.1.2.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- NT ACLs may be bypassed by booting an alternative operating system.
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

### 6.1.3. Delete \$WinNT\$.inf files

ID	Version	Level	Enforcement
NT4GEN-SETUP-4	1.0	baseline	mandatory

#### 6.1.3.1. Standard

For unattended setups the \$WinNT\$.inf file should be deleted.

#### 6.1.3.2. Detailed Steps

- Ensure any \$WinNT\$.inf files are removed after an unattended installation.

#### 6.1.3.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- The username and password of the user used to add the machine to the domain may be exposed.
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

### 6.1.4. Installation disk image duplication

ID	Version	Level	Enforcement
NT4GEN-SETUP-5	1.0	baseline	mandatory

### 6.1.4.1. Standard

Do not install by duplicating a previous disk image, unless the disk image copy tool used is NT-aware and capable of assigning a unique machine SID after duplication.

### 6.1.4.2. Detailed Steps

- Do not install using a disk image duplication.
- Or, if using disk image duplication, ensure that the disk image duplication tool is NT-aware and able to assign unique machine SIDs after duplication.

### 6.1.4.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Machines and user accounts will have duplicate SIDs, undermining the security enforcement of NT.
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

## 6.1.5. Format all disk partitions with NTFS

ID	Version	Level	Enforcement
NT4GEN-SETUP-1	1.0	baseline	mandatory

### 6.1.5.1. Standard

All filesystem partitions must be formatted prior to installation as NTFS.

### 6.1.5.2. Detailed Steps

- Choose Format as NTFS from setup menus.
- Do not use FAT partitions during installation, format as NTFS during installation.

### 6.1.5.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Filesystems will not be protected by NT ACLs.
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

### **6.1.6. Do not use HPFS or FAT file structures. Always use NTFS.**

<b>ID</b>	<b>Version</b>	<b>Level</b>	<b>Enforcement</b>
NT4GEN-SETUP-6	1.0	baseline	mandatory

#### **6.1.6.1. Standard**

Do not use HPFS or FAT file structures. Always use NTFS.

#### **6.1.6.2. Detailed Steps**

- Opt for using NTFS alone during system commissioning

#### **6.1.6.3. Risks Addressed**

Where this control is not applied, the following residual risks exist:

- Other file structures do not consistently support windows NT access control
- The use of other file structures may be used to subvert security controls
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

---

# Chapter 7. Auditing and Monitoring

## 7.1. Audit log destination and format

### 7.1.1. Security event logging must be enabled and not set to overwrite events

ID	Version	Level	Enforcement
NT4GEN-AUDIT-4	1.0	baseline	mandatory

#### 7.1.1.1. Standard

Security event logging must be enabled and not set to overwrite events

#### 7.1.1.2. Detailed Steps

- Switch security event logging on
- Configure event logging so as not to overwrite events

#### 7.1.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Reconstruction of a sequence of a sequence of events requires events to be recorded
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

## 7.2. Events to be audited

### 7.2.1. Set up file auditing for group everyone

ID	Version	Level	Enforcement
NT4GEN-AUDIT-3	1.0	baseline	recommended

#### 7.2.1.1. Standard

File auditing for group everyone should be set up to record failed attempts for read, write, execute and success and failure for delete, change permissions and take ownership.

### 7.2.1.2. Detailed Steps

- Set up file auditing for group everyone as follows;
- Read - Audit failed attempts
- Write - Audit failed attempts
- Execute - Audit failed attempts
- Delete - Audit failure and success
- Change Permissions - Audit failure and success
- Take Ownership - Audit failure and success

### 7.2.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Reconstructing a sequence of events requires certain events to be recorded
- Failing to record certain events may allow a breach or a failure to go undetected
- Failing to record certain events may prevent successful recovery from a breach or a failure
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

## 7.2.2. Set up directory auditing for group everyone

ID	Version	Level	Enforcement
NT4GEN-AUDIT-2	1.0	baseline	mandatory

### 7.2.2.1. Standard

Set up directory auditing for group everyone such that failed attempts are recorded for read, write, execute and failed and successful attempts are recorded for delete, change permissions and take ownership.

### 7.2.2.2. Detailed Steps

- Set up directory auditing for group everyone as follows;

- Read - Audit failed attempts
- Write - Audit failed attempts
- Execute - Audit failed attempts
- Delete - Audit failure and success
- Change Permissions - Audit failure and success
- Take Ownership - Audit failure and success

### 7.2.2.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Without an audit trail of activity reconstructing misuse cannot be achieved
- A loss of accountability may occur
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

## 7.2.3. Network alerts must be enabled for excessive login failures

ID	Version	Level	Enforcement
NT4GEN-AUDIT-5	1.0	baseline	mandatory

### 7.2.3.1. Standard

Network alerts must be enabled for excessive login failures

### 7.2.3.2. Detailed Steps

- Configure network alerts for excessive login failures

### 7.2.3.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Non-interactive/network login failures may be indicative of an attack
- Non-interactive/network login failures may be indicative of a failed service

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

## **7.2.4. The audit policy must be set up to record failure and success for Logon and Logoff, User and Group Management, Security Policy Changes, Restart, Shutdown and System and failure for File and Object Access**

<b>ID</b>	<b>Version</b>	<b>Level</b>	<b>Enforcement</b>
NT4GEN-AUDIT-1	1.0	baseline	mandatory

### **7.2.4.1. Standard**

The audit policy must be set up to record failure and success for Logon and Logoff, User and Group Management, Security Policy Changes, Restart, Shutdown and System and failure for File and Object Access

### **7.2.4.2. Detailed Steps**

- Set up audit policy as follows;
- Logon and Logoff Audit failure and success
- File and Object Access Audit failure
- User and Group Management Audit failure and success
- Security Policy Changes Audit failure and success
- Restart, Shutdown and System Audit failure and success

### **7.2.4.3. Risks Addressed**

Where this control is not applied, the following residual risks exist:

- Capturing events allows an audit trail of activity to be created
- A failure to capture events prevents abnormal activity from being identified
- This allows an attackers behaviour to go unnoticed.
- Failing to record security events may result in a loss of accountability
- A loss of accountability makes it difficult to determine the nature of a breach

- This may result in regulatory compliance breaches
- This may make legal action problematic to pursue
- This may make reconstructing the system securely difficult to achieve
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

## 7.2.5. Set up registry key auditing for group everyone

ID	Version	Level	Enforcement
NTGEN-AUDIT-4	1.0	baseline	recommended

### 7.2.5.1. Standard

Registry key auditing should be set up to not audit query value, create subkey, read control, to audit successful attempts to set value, enumerate subkeys, notify, create link, delete and to audit successful and unsuccessful attempts to write DAC

### 7.2.5.2. Detailed Steps

- Set up registry key auditing as follows;
- Query Value - Not audited
- Set Value - Audit successful attempts
- Create Subkey - Not audited
- Enumerate Subkeys - Audit successful attempts
- Notify - Audit successful attempts
- Create Link - Audit successful attempts
- Delete - Audit successful attempts
- Write DAC - Audit successful and unsuccessful attempts
- Read Control - Not audited

### 7.2.5.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Reconstructing a sequence of evnts requires events to be recorded

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

# Chapter 8. Checklist

<i>User Configuration</i>		
<i>User Administration</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
NT4GEN-U C-1	Is access to login scripts and profiles restricted only to their user and administrators?	
<i>Default Accounts</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
NT4GEN-D A-2	Has the administrator account been renamed to an attributable account name and the password changed?	
NT4GEN-D A-1	Has the guest account been disabled?	
<i>Privileges</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
NT4GEN-PR IV-13	Is the advanced user right to load and unload device drivers assigned to any users?	
NT4GEN-PR IV-7	Is the advanced user right to create a page file assigned to any users?	
NT4GEN-PR IV-6	Is the advanced user right to bypass traverse checking assigned to any users?	
NT4GEN-PR IV-16	Is the advanced user right to profile single process assigned only to administrators?	
NT4GEN-PR IV-19	Is the advanced user right to replace a system level process token assigned to any user?	
NT4GEN-PR IV-9	Is the advanced user right to create permanent shared objects assigned to any users?	
NT4GEN-PR IV-11	Is the advanced user right to generate security audits assigned to any users other than the administrators or security users?	
NT4GEN-PR IV-10	Is the advanced user right to debug programs assigned only to administrators and developers?	
NT4GEN-PR IV-4	Is the user right to shutdown the system assigned to local groups and not to individual users?	
NT4GEN-PR IV-17	Is the advanced user right to profile system performance assigned only to administrators?	
NT4GEN-PR IV-18	Is the advanced user right to receive unsolicited device input assigned to no users?	
NT4GEN-PR IV-2	Is the user right to force shutdown from a remote system assigned to local groups and not to individual users?	
NT4GEN-PR IV-12	Is the advanced user right to increase scheduling priority assigned only to administrators?	

Checklist

NT4GEN-PR IV-15	Is the advanced user right to modify firmware environment variables assigned only to administrators?	
NT4GEN-PR IV-5	Is the advanced user right to act as part of the operating system assigned to any one?	
NT4GEN-PR IV-8	Is the advanced user right to create a token object assigned to any users?	
NT4GEN-PR IV-3	Is the user right to logon locally assigned to local groups and not to individual users?	
NT4GEN-PR IV-1	Is the user right to change the system time assigned to local groups and not to individual users?	
NT4GEN-PR IV-14	Is the advanced user right to logon as a service assigned only to administrators?	
<i>Security Compliance</i>		
<i>Security Management</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
NT4GEN-VI RUS-1	Is ant-virus software installed and maintained on all machines?	
NT4GEN-LE GAL-1	Ensure that a legal notice appropriate to your jurisdiction is displayed in the legal notice placeholder for display prior to logon	
<i>Network Security Configuration</i>		
<i>Network Interface Considerations</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
NT4GEN-NE TW-1	Is FTP installed or if part of the default image is it disabled?	
<i>Configuration</i>		
<i>Files and File Permissions</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
NT4GEN-FI LE-1	Are sensitive data files encrypted?	
<i>Administration</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
NT4GEN-A DM-1	Has clearing of the system page file at shutdown been enabled?	
<i>Installation</i>		
<i>Setup Choices</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>

Checklist

NT4GEN-SE TUP-2	Is NT the only operating system installed?	
NT4GEN-SE TUP-3	Has access to alternative boot mechanisms been physically and/OR BIOS password restricted?	
NT4GEN-SE TUP-4	For unattended setups, has the \$WinNT\$.inf file been deleted after installation?	
NT4GEN-SE TUP-5	For installations using disk image duplication, has the machine been assigned a unique SID?	
NT4GEN-SE TUP-1	Are all partitions formatted as NTFS?	
NT4GEN-SE TUP-6	Are there any FAT or HPFS partitions on the system?	
<i>Auditing and Monitoring</i>		
<i>Audit log destination and format</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
NT4GEN-A UDIT-4	Is security event logging enabled and set so as not to overwrite events?	
<i>Events to be audited</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
NT4GEN-A UDIT-3	Has file auditing been set up for group everyone?	
NT4GEN-A UDIT-2	Has directory auditing for group everyone been set up in accordance with policy?	
NT4GEN-A UDIT-5	Are network alerts enabled for excessive login failures?	
NT4GEN-A UDIT-1	Has the audit policy been set up to record the events defined in the audit policy?	
NTGEN- AUDIT-4	Has registry key auditing been set up in accordance with policy?	