

# **NT4 Workstation Security Standard**

---

# NT4 Workstation 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 implementations that are part of a domain.

This standard contains 3 baseline controls, and 0 above baseline controls, for a total of 3 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. Privileges .....	4
2.1.1. The user right, access this computer from the network, should be available to everyone .....	4
3. Configuration .....	5
3.1. Files and File Permissions .....	5
3.1.1. Show common program groups .....	5
3.1.2. Disable run on the file menu .....	5
4. Checklist .....	7

---

# 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 workstations.
- To provide guidance to administrators, developers and security personnel in securely implementing <trademark>Microsoft</trademark> <trademark>Windows</trademark> NT4.0 workstations.

## 1.2. Scope

Controls specified in this document apply to workstation implementations of NT4.0 that are 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 workstation standard. Controls specific to server or domain controller implementations are not defined here but will be the subject of additional standards. This document should also be read in conjunction with the NT 4 generic security standard, which specifies controls applicable to all NT4 implementations.

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 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 believe 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. Privileges

### 2.1.1. The user right, access this computer from the network, should be available to everyone

ID	Version	Level	Enforcement
NT4W-PRIV-1	1.0	baseline	recommended

#### 2.1.1.1. Standard

The user right, access this computer from network should be available to everyone

#### 2.1.1.2. Detailed Steps

- Ensure that the everyone group holds the user access right, access this computer from the network.

#### 2.1.1.3. Risks Addressed

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

- Business information and applications may be unavailable.

---

# Chapter 3. Configuration

## 3.1. Files and File Permissions

### 3.1.1. Show common program groups

ID	Version	Level	Enforcement
NT4W-USER-2	1.0	baseline	recommended

#### 3.1.1.1. Standard

Show common program groups

#### 3.1.1.2. Detailed Steps

#### 3.1.1.3. 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.

### 3.1.2. Disable run on the file menu

ID	Version	Level	Enforcement
NT4W-USER-1	1.0	baseline	recommended

#### 3.1.2.1. Standard

Disable run on the file menu

#### 3.1.2.2. Detailed Steps

- The standard workstation image should be built with this option unavailable

#### 3.1.2.3. 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.

---

# Chapter 4. Checklist

<i>User Configuration</i>		
<i>Privileges</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
NT4W-PRIV-1	Is the user right, access this computer from network, available to everyone?	
<i>Configuration</i>		
<i>Files and File Permissions</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
NT4W-USE R-2	Are common program groups shown?	
NT4W-USE R-1	Is run disabled on the file menu?	