



Document type: Example

(Removable front sheet)

Outline security policy for a WARP service

(V3.0) July 2006

Keywords

[Policy, Security]

Important notice

This document provides an example of an outline security policy for a WARP Provider who wishes to implement the types of services described in the WARP Toolbox. It is not intended to be a definitive policy, but rather an outline describing those aspects of good practice that will ensure that WARP services are developed, provisioned and operated in a secure manner.

It is recommended that this example document be edited to produce one which best meets the emerging WARP's specific needs and to which their particular community naming/branding may be applied. This front sheet should therefore be removed and should not form any part of the final document. The WARP Toolbox logo on the next page should be replaced with that of the new WARP if that page is required.

The format of this document is consistent with the WARP Toolbox series of MS Word document templates, which are available as downloads from the WARP Toolbox site.

Version control

This document may be made available in more than one electronic version or in print. In a case of existing or perceived difference in contents between such versions, the reference version is the version available for download from the WARP Toolbox site <http://www.warp.gov.uk>

If you find errors in the current document, please send your comment to: editor@warp.gov.uk

Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by NISCC. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes. NISCC shall also accept no responsibility for any errors or omissions contained within this document. In particular, NISCC shall not be liable for any loss or damage whatsoever, arising from the usage of information contained in this document.

Copyright notification

The copyright and the foregoing restrictions, extend to reproduction in all media. The rights to modify and reproduce are described in the WARP Toolbox terms and conditions described on the WARP Toolbox site.

Outline security policy for a WARP service

Version: V<x.x>
Date: <Mth yyyy>
Author: <Author>

You can replace this logo with your own if you wish to use this page



Contents

1	Scope.....	2
2	Definitions.....	2
3	Background	2
4	Policy statements.....	3
4.1	Physical security	3
4.2	System access controls.....	3
4.2.1	Network access	3
4.2.2	User access	4
4.3	Data encryption.....	4
4.4	Data protection.....	5
4.5	Operation security.....	5
5	History.....	6

1 Scope

This document provides an overview of the key security measures that should be taken to ensure that the WARP deployment:

- i. employs 'good practice' protection from Internet-borne attack, either deliberate or via automated means.
- ii. correctly controls WARP members and administrator access to a WARP system.
- iii. protects data stored within the WARP system to ensure that WARP members may report sensitive information with confidence.

These measures relate to the three core WARP services: Filtered Warnings; Trusted Sharing and Advice Brokering. This policy document has been kept deliberately brief, in order to highlight the key points without recourse to minutia that could detract from its purpose.

2 Definitions

For the purposes of this document, the following terms and definitions will apply:

- **WARP Server** A Windows 2003 server, running IIS, SQLServer 2000 and SQL Server Notification Services, that may be accessed via the Internet.
- **WARP Server Administrator** An authorised person with administration access to the operating system of the WARP Server.
- **WARP Administrator** An authorised person having 'master' access to the WARP server and responsibility for managing WARP membership and content. This person is also likely to be the owner of this security policy.
- **WARP Member** An authorised WARP user who receives alerts and contributes information.

3 Background

A successful WARP is based on the building and maintenance of trust within the user community. It is therefore vital that the confidentiality, integrity and availability of the user member's information, and the WARP systems, are safeguarded by effective security measures. To this end, an effective and usable Security Policy will form the cornerstone of the WARP security measures. However, at the time of the preparation this document, no suitable common, standard has been identified. This in turn has necessitated the preparation of this Outline Security Policy, based on the example within the WARP Toolbox.

4 Policy statements

4.1 Physical security

In order to operate a WARP, at least one WARP server will be required within each WARP community of interest. Physical access to the WARP server must be tightly controlled, since physical access to the WARP Server will enable unauthorised persons to input and/or extract data. It is envisaged that most WARP servers will be located within ISP (Internet Service Provider) facilities, but this is not essential. However, as a minimum, the host environment should provide the following security features:

- Secure premises, with access control limited to authorised personnel displaying formal security passes.
- 24 Hour access control, via an unattended biometric verification system, or an attended security guard.
- Resilient power supplies supplied by diverse feeds, protected by generator and battery back-up systems.
- Individual server access logs (to provide the host organisation with knowledge of which personnel accessed a system on an individual server basis).
- Secure storage of back-up media.

Whilst it is not always possible to dictate the physical security arrangements for WARP Members and Administrators, care must be taken to ensure that the physical compromise of their environment does not lead to the compromise the WARP system (e.g. should a WARP Member's laptop computer be lost, or stolen, possession of the computer alone will not enable a third party to access the WARP System).

4.2 System access controls

4.2.1 Network access

Network access to the WARP Server (by means of the Internet, or an internal communications network) must be protected behind a Firewall. The Firewall must be capable of:

- Logging all network communications and storing the resultant data for at least six months and
- Making log data available to the WARP Administrator should he/she require access to it.

Access to the Firewall information log should be restricted to WARP Server Administrators and WARP Administrators.

The Firewall will be configured to permit only those network connections that are required to enable the WARP to function properly. For example, a Firewall configuration may be specified as follows:

- Inbound access to the WARP server will be restricted to HTTPS (TCP port 443). Should remote management of the WARP server be required, this will be limited to either:
 - the use of SSH (TCP port 22) and/or Windows RDP (TCP port 3389), where both SSH and RDP access will be restricted to known IP addresses. (Note: Windows 2003 does not include a SSH server, but versions are available from third parties)
 - a VPN solution that provides additional authentication using digital certificates, or authentication tokens.
- Outbound access from the WARP must be limited to SMTP (TCP port 25), DNS (UDP and TCP port 53) and HTTPS (TCP port 443). The HTTPS access is required only for peer-to-peer connections, and should be restricted to a limited number of destination addresses.

The web server installation on the WARP Server will be further protected using an application firewall or intrusion prevention system, in order to block attacks using TCP port 443.

4.2.2 User access

WARP Server Administrator accounts must be strictly limited and unique (the use of generic Administrator accounts will not be permitted). The WARP Administrator must maintain a record of the WARP accounts that have been issued to Members. Where an ISP manages the WARP Server, the procedures employed for the handling of Administrative access must be reviewed periodically to ensure they remain robust.

Access to the WARP System shall be controlled via user accounts, which are created by the WARP Administrator. There will be no “self registration” process. All WARP member accounts must be specifically registered by the WARP Administrators to known individuals within the membership community. The FWA signup request system conforms to this policy, as a WARP Administrator must approve all new accounts.

E-mail delivery failures received by the WARP system in response to mailed alerts, will be investigated by the WARP Administrator – this mechanism will help to ensure that accounts are deactivated when a WARP member leaves the community and ‘moves on.’

4.3 Data encryption

All data transferred between the WARP Administrator/Member’s web browser and the WARP Server must be encrypted via SSL employing a minimum 128-bit RC4 cipher. WARP users must take care to ensure their browsers will not cache encrypted pages¹.

Sensitive data stored within the WARP Server must be encrypted prior to being recorded on tape for back-up purposes. The encryption keys used for this purpose must be held by the WARP Administrators, allowing them to recover the encrypted data should the WARP Server be rendered unavailable.

¹ Internet Explorer users can ensure this by selecting “Tools->Internet Options”, going to the “Advanced” tab, scrolling down to the “Security” section and ticking “Do not save encrypted pages to disk”.

Remote Management connections, by any method permitted in section 4.2.1, will be encrypted using the 3DES or AES ciphers.

4.4 Data protection

WARP Server Administrators have no requirements for an account to access the WARP system, however it should be noted that they can access and alter any data held on the server, and the use of such accounts must therefore be tightly controlled.

The WARP Administrator is empowered to view and update all WARP data. WARP Members may only update their own profile, contribute information and read all published information. An exception shall be permitted with regard to the multi-user bulletin board, where access may be restricted to specified WARP Members.

In circumstances where the submission of information by a WARP Member concerning a 'compromise' might be regarded as 'sensitive' to that member's organisation, the member may submit the information anonymously. The information given will be restricted to the WARP Administrator, with no other WARP Member being privy to the source. These reports will, however, have a log number, which the WARP Administrator may use to trace the originating source.

Data held within the WARP system will be used only in accordance with the WARP Privacy Policy.

4.5 Operation security

The WARP System will distribute e-mail warnings and advisories (content) provided by the WARP Administrators. E-mails sent by the WARP system will be digitally signed to allow their authenticity to be verified by the WARP Members.

No direct instructions will be issued to WARP members via the e-mail alerts, rather the e-mails will be used to provide brief information and advise where full information can be obtained. Any e-mails claiming to be from the WARP Service that are either not signed, or give instructions to the WARP Members to take direct action, should be treated as suspicious and the WARP Administrator notified accordingly.

The WARP Administrators have no access to a WARP Member's password, and have no reason to request it. A WARP Member therefore should not divulge his/her access information to anyone else. Should a WARP member forget his/her password, the WARP Administrator will reset it.

The WARP Server Administrator must implement all security patches published by the software vendors in a timely manner.

5 History

Version	Date	Description
V1.0	Dec 2003	First issue WARP Toolbox example for an Outline Security Policy
V2.0	June 2004	Standard WARP Toolbox template applied
V3.0	July 2006	Content of the example updated to reflect latest software versions