



## Information Security Policy

For further information please contact:

**Melanie Jones**

Project Manager - Information security services

[melanie.jones@mycci.co.uk](mailto:melanie.jones@mycci.co.uk)

+44 (0) 1484 438800

[www.mycci.co.uk](http://www.mycci.co.uk)

## Contents

1	Introduction .....	3
2	Definitions .....	3
3	Backgrounds.....	3
4	Policy Statements .....	4
4.1	Physical Security .....	4
4.2	System Access Controls .....	4
4.2.1	Network Access.....	4
4.2.2	Users Access .....	5
4.3	Data Encryption.....	5
4.4	Data Protection .....	5
4.5	Operational Security.....	6

## **1 Introduction**

This document provides an overview of the key security measures which have been taken to ensure that **MYWARP** –

- Employs good-practice protection against internet-borne attack
- Correctly controls and manages Member and Administrator access to the **MYWARP** system
- Protects data stored within the **MYWARP** system, ensuring that Members can report sensitive information with confidence

These measures relate to the three core **MYWARP** services: Filtered Warnings; Trusted Reporting and Advice Brokering. This policy document is deliberately brief, covering the key points without going into technical details.

## **2 Definitions**

For the purposes of this policy document the following definitions apply:

- **MYWARP Server**
  - A Windows 2003 server, running IIS, SQL Server 2003 and SQL Server Notification Services, which may be accessed via the Internet
- **MYWARP Server Administrator**
  - An authorised person with administration access to the operating system of the **MYWARP** server
- **MYWARP Administrator**
  - A senior authorised person with ‘Master’ access to the operating system of the **MYWARP** server, and responsible for managing membership and content. The ‘owner’ of this security policy.
- **MYWARP Member**
  - An authorised **MYWARP** user who receives alerts and contributes information.

## **3 Backgrounds**

**MYWARP** depends on the building and maintenance of trust within the **MYWARP** Community. It is therefore vital that the confidentiality, integrity and availability of the user Members’ information and the **MYWARP** system are safeguarded by adequate security measures. To this end, an effective and usable security policy forms the cornerstone of **MYWARP** security measures.

## 4 Policy Statements

### 4.1 Physical Security

As physical access to the **MYWARP** server could enable unauthorised persons to input, extract or corrupt data, it is tightly controlled. The server is hosted by **MYCCI**, a BS:7799 Certified enterprise, and the following security measures apply:

- Secure premises, with access limited to authorised personnel. A formal system of Visitor Passes and controls is in place
- A secure, locked Server Room, with access by authorised, key-holder staff only, and for logged visitors accompanied by such staff
- A secure, locked Server Cabinet, with access limited to three authorised, key-holding Network Administrators
- Resilient mains power supply on a separate circuit, with regularly tested Uninterruptible Power Supply back-up system
- Individual Server Access Logs
- Secure storage of back-up media

### 4.2 System Access Controls

#### 4.2.1 Network Access

Network access to the **MYWARP** server, by means of the Internet or an internal communications network, is protected behind an externally managed Firewall. All network communications are logged and the resultant data is stored for a minimum of six months, during which time the data is available to the **MYWARP** Administrator.

Access to the Firewall Log is restricted to **MYWARP** Server Administrators and Administrators. The firewall is configured to permit only those network connections which are required to enable the correct functioning of **MYWARP**.

The web server installation on the **MYWARP** Server was carefully protected using and application firewall, in order to block attacks using TCP port 443.

#### **4.2.2 Users Access**

**MYWARP** server Administrator accounts are strictly limited and unique. The use of generic Administrator Accounts is not permitted. The **MYWARP** Administrator maintains a record of the **MYWARP** accounts which have been issued to members. Access to the system is controlled by user accounts, which are created by the **MYWARP** Administrator. There is no 'self-registration' process. All **MYWARP** Member Accounts are specifically registered by the **MYWARP** Administrator to named individuals within the membership community.

E-mail delivery failures received by the **MYWARP** system in response to mailed alerts will be investigated by the Administrator, which will help to ensure that Member Accounts are de-activated when a **MYWARP** member leaves the community.

#### **4.3 Data Encryption**

All data transferred between Administrator's or a Member's web browser and the **MYWARP** Server will be encrypted via SSL employing a minimum 128-bit RC4 cipher. Users must ensure that their browsers will not cache encrypted pages.

Sensitive data stored on the **MYWARP** Server is encrypted before being recorded on tape for back-up purposes. The encryption keys are held by the Administrators, so that encrypted data can be recovered in the event of the **MYWARP** Server becoming unavailable.

#### **4.4 Data Protection**

**MYWARP** operations will comply with the Data Protection Act 1998 and related legislation. The **MYWARP** Administrator can view and up-date all **MYWARP** data. Members can read all published information and can contribute information, but can only up-date their own profile. Access to the multi-user bulletin board may be restricted to specified Members.

In circumstances where a submission by a Member concerning a 'compromise' may be regarded as 'sensitive' to the Member's organisation, the information may be submitted anonymously. Such reports will have a log number, which will allow the **MYWARP** Administrator to identify the originator, but Members will not have access to the identity of the source.

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

#### **4.5 Operational Security**

The **MYWARP** system will distribute e-mail warnings and advisories provided by the **MYWARP** Administrator. E-mails sent by the **MYWARP** system are digitally signed to allow their authenticity to be verified by Members.

Direct instructions will not be issued to Members via the e-mail alerts. They will provide brief information, and advise where full information can be obtained. Any e-mails purporting to come from the **MYWARP** system which are either not digitally signed or give Members instructions to take direct actions must be treated as suspicious, and the **MYWARP** Administrator must be notified immediately.

The **MYWARP** Administrator has no access to any Member's password, and has no reason to request it. Members must not divulge their access information to anyone. If a Member should forget a password, then a **MYWARP** Server Administrator can re-set it.

All software patches and similar updates provided by the software supplier will be evaluated for relevance and criticality, and installed promptly by a **MYWARP** Server Administrator when necessary to ensure that the system meets optimum security requirements.