# AusCERT Policies

## Overview

These AusCERT Policies are referenced in the AusCERT Membership and Services Terms, dated 9 December 2014.

## Third Party Intellectual Property Policy

AusCERT External Security Bulletins contain third party Intellectual Property. ESBs are distributed with permission from the third parties and the source of the material is identified in the ESB. Third parties retain all intellectual property rights in their content and the licence provided under the AusCERT Membership and Services Terms does not include third party content. Your rights to use third party intellectual property are governed by the terms of use that accompany, or are referred to in, the original version of that third party content.

## Domain Policy

AusCERT records members' domains and IP addresses for the purposes of providing proactive incident response services to members. AusCERT checks the ownership of a member's domains before we associate the domain with the member through a whois lookup. In cases where the whois record shows that the domain is not owned or controlled by the member, then we will request members take the following action to prove their ownership; or authority to include the domain for monitoring purposes. Either:

a) Contact the domain registrant and ask that they transfer the domain to the member; or
b) Obtain a domain authority letter (DAL) from the domain registrant, on its letterhead, addressed to AusCERT with the words:

    Dear AusCERT
    *I am an authorised employee of* [insert company or organisation that is the registrant of the domain], *and as such, authorise AusCERT to monitor the domain* [insert domain] *for the purposes of providing security services to* [insert member organisation's name].

Notify AusCERT by sending an email to membership@auscert.org.au when (a) or (b) is completed. Where a member cannot provide proof of ownership or proof of authorisation, AusCERT reserves the right to reject the domain.

## Confidentiality Policy

In order to provide services to our members, we collect and receive reports about information security incidents affecting our members systems, domains or IP addresses. In order to provide these services, sometimes it is necessary for AusCERT to contact other parties in relation to an incident, such as the alleged attacking site, an Internet service provider, an overseas computer security incident response team (CSIRT) etc.

In cases where the member has experienced an incident, AusCERT will not disclose details of the incident or the member to a third party unless permission has been granted by the member for the purpose of providing assistance to the member to resolve or mitigate the incident. Additionally, where

possible, details about the incident will be sanitised to minimise the amount of information passed about a system/organisation which has been affected.

We also collect information about computer security incidents which are sent to us for information only. In order to better inform our members with regard to the nature of computer security threats, AusCERT draws upon aggregated computer security incident data we hold to assess the likely impact of current or ongoing threats, to identify changing trends and understand the nature of computer attack related activity. Where appropriate we incorporate our analysis of general trends and activity into our security bulletins and other publications or advice. In drawing upon aggregated incident data in this way, we will not divulge identifying details about members such as their domains, IP addresses, personnel or organisation.

If you wish to send encrypted email to us, please use our PGP key, available from https://auscert.org.au/1922. Please provide your PGP key or digital certificate so may reply securely.

## Privacy Policy

In accordance with Queensland government's Information Privacy Principles (in its Information Privacy Act 2009), this Policy explains how we deal with the privacy of the personal identifying information we collect in the course of performing providing services to our members.

AusCERT collects and holds personal identifying information about its member contacts for the purpose of providing services to members.

AusCERT also receives personal identifying information from people and organisations, who are not members, who report computer security incidents to AusCERT.

Whether a member or not, AusCERT may pass a person's name and contact details to appropriate third parties for the purpose of providing incident management services in relation to the incident, with the person's consent, but will not otherwise pass their personal details to other third parties, except in accordance with the AusCERT Membership and Service Terms.

AusCERT adopts multiple mechanisms (through the use of technologies, policies, practices and procedures) to secure its network and the sensitive and personal information stored on it, or otherwise held in our possession.

# Information Handling and Sharing Policy

Sometimes AusCERT receives information from trusted sources about new vulnerabilities, threats or incidents which AusCERT is permitted to pass to its members. Depending on the source and sensitivity of the information, there may be restrictions on how the information can be used or distributed by the member. If you receive information from AusCERT with the following handling caveats, then you agree to handle the information in accordance with this Policy.

| Traffic Light Protocol Handling Label | Description | Example |
|---|---|---|
| TLP: WHITE | The content can be distributed publicly if the source of the information is retained. | |
| TLP: GREEN | This is general member only content and not for further distribution beyond the member organisation and its authorised personnel or contractors.<br><br>This is not public information but can be shared widely within the member organisation if the source of the information is retained. | Most member-only content on the AusCERT web site of a generic nature should be regarded as GREEN, except for member-specific information. |
| TLP: AMBER | This is general member only content which, due to its sensitivity, should only be distributed within the member organisation, on a strictly need-to-know basis and the source and handling caveats must be retained. | Information sent to the auscert-contact alias may be classified as AMBER. |
| TLP: RED | This is general member only content which, due to its extreme sensitivity should not be distributed further, including within the member organisation. | Information sent to specific email recipients is classified as RED unless explicitly stated otherwise. |