



UNIVERSITY OF TASMANIA | PROCEDURE DOCUMENT – No. 2.0

SPAM Prevention Procedure

Procedure Scope	University wide.
Commencement Date	1 October 2004.
Review Date	<i>Feb 2005.</i>
Organisational Unit responsible for day-to-day operation of the procedure	Unit name: IT Resources Phone: x6336 Fax: x7171 Email: IT.Enquiries@utas.edu.au

Procedure

1 Purpose

The implementation of a high-performance anti-spam application designed to protect the enterprise from the transmission of spam.

Spam prevention applications provide for the establishing of baseline settings for the tagging of emails, as further detailed in section 7.

Default Position:

- a) The baseline detection setting is to be set at Level 5 or ‘aggressive’, the second highest level.
- b) The Commercial Offer filter detection setting is to be set to Level 3 or ‘high’.
- c) All email will be scanned and possibly tagged as spam should it fall within categories identified in Section 7.

2 Exceptions

Applies, in the first instance, to all University of Tasmania members using email clients that allow filtering on email header information. Users may individually choose not to use the filtering capabilities documented and, as such, choose to “opt out” and not undertake spam filtering by way of their email client.

3 Definitions and Acronyms

“ <i>UTas</i> ”	University of Tasmania.
“ <i>Senior Managers</i> ”	Refers to Heads of School and Heads of Section.
“ <i>Service Desk staff</i> ”	Refers to staff employed on the Library managed Service (sic. Help) Desk

4 Links to Related Forms, Records and Electronic Databases

[SPAM Prevention – User Documentation](#)

5 Detailed Steps, Procedures and Actions

Separate user documentation detailing filter rule creation within individual email clients has been produced. The documentation covers numerous email clients:

- Lotus Notes
- Eudora
- Microsoft Outlook
- Entourage (Macintosh)
- Apple's Mail (Macintosh)

6 Key Words

Procedures will be housed on the UTas web site. Identifying key words will assist students and staff to locate the relevant policy using the 'search' function.

- SPAM
- Trend Micro
- IMSS
- Filter

7 Supporting Documentation

Trend Micro™ Spam Prevention Solution is a high-performance anti-spam application designed to protect the enterprise from spam at the gateway. It is integrated with Trend Micro™ InterScan Messaging Security Suite (IMSS), which provides comprehensive messaging security – antivirus, content filtering, and anti-spam — in one easy-to-manage platform.

Spam Prevention Solution is designed to defeat spam using heuristics rules technology—a technology that offers more adaptable and “future-proof” protection against the ever changing tactics of spammers.

Policy-based configuration options allow University administrators to assign variable catch rate sensitivities based on spam category and user groups, along with flexible Filter Actions for appropriate message disposition options. Spam Prevention Solution can delete, quarantine, tag based on spam likelihood level.

Heuristics rules technology monitors, evaluates, and identifies suspicious email traffic to determine a spam probability based upon collectively weighted and contextually evaluated characteristics. Testing was undertaken to ensure the product would provide the University with maximum spam capture rates with low false positives.

As messages pass through the system, the SPS heuristic filter applies thousands of rules against the message envelope, the header, and the content. Each rule is assigned a numerical value, and an equation is formulated based on the weighted significance and the combination of rules that are triggered. The result of this equation is the spam score.

SPS makes a decision on whether the message is spam or valid by measuring the spam score against the desired level of spam sensitivity. Setting the sensitivity higher causes more messages to be considered spam, since increased sensitivity means that a lower spam score will result in a message being considered spam. Administrators can set the overall sensitivity of the heuristic spam filters, as well as fine-tune the sensitivity to different categories of spam. If the heuristic spam filter categorises a message as spam, it will usually fall into one of four categories:

- Sexual content: Adult or pornographic material
- Racist content: Racially insensitive material
- Make Money Fast: Get-rich-quick material
- Commercial offer: Sale notices, coupons, and special offers

If the spam score for a given message exceeds the sensitivity level of the policy, the message is considered spam. There are three exceptions to this:

- If the sender appears on the **Approved Senders** list, the message is never considered spam.
- If the sender appears on the **Blocked Senders** list, the message is always considered spam.
- If text in the message triggers a **Text exemption filter**, the message is never considered to be spam.

Responsibilities

Implementation	Director, IT Resources.
Compliance	All UTas Staff and Students.
Development/Review	Director, IT Resources.
Interpretation and Advice	Manager, Computing & Distributed Systems.
Data Collection and Analysis	Team Leader, Systems / Team Leader, Desktop Management Systems.

Who Should Know this Procedure?

- Senior Managers
- Lecturers / Tutors
- Service Desk staff
- All Staff & Students

Effectiveness of this Procedure

- Reduction in queries received by the Service Desk on Spam related issues.

Procedure History

Revision Ref. No.	1.0
Approved or Rescinded	Executive Director, Finance and Administration
Date	xx/xx/xx
Committee/ Board	
Resolution Number	