



For the definitions of terms used in this policy document refer to the Delegations of Authority. Senior Delegated Officer (SDO) means the manager with the delegated authority for the management of a number of organisational units and/or University wide function(s), ie the relevant DVC or PVC (College). As appropriate for the local nomenclature and reporting lines, when this document refers to Department read also School or Unit; to Faculty read also: Sydney College of the Arts, Sydney Conservatorium of Music or Administrative Unit; to Head read Head of Department/School/Unit; and to Dean read also Director or College Principal. For Head, Dean and PVC read also HOA, Senior Manager and DVC, as appropriate

1 Background

Computers, especially department servers, desktop and laptop computers, can be compromised by attacks from computer viruses. These can be widely spread via email messages processed via unprotected University computers.

To assist in combating this problem the University has implemented virus scanning systems for receipt of emails on University-wide and Departmental mail servers. This protection is designed to supplement, but not change, the continuing need for individual computer users to protect their local University computer resources from virus attacks, spread by e-mail or any other method.

2 Policy

The University requires all email messages carried over its networks (including messages sent from the outside, internally, and to the outside) to be scanned for computer viruses. The University asserts its right to delete or alter messages that, in its discretion, are suspected of containing viruses.

3 Scope and Limitations

This policy applies to all e-mail received or sent through University owned or operated email servers.

Whilst the University takes all reasonable steps to ensure that legitimate, legal messages are delivered in a timely manner, users are reminded that the email service is not a “guaranteed delivery” medium.

4 Definitions

Defanging content

Rendering an email message or attachment harmless.

Refanging content

A process to restore an email attachment to its original state as a file on a computer system.

Email scanning

Examining an email message and/or attachment for suspicious content.

Email cleaning

Removing a virus and all traces of it from an email message.

Email Virus

Malicious executable or potentially executable code carried in email messages. When received on a computer, alters the configuration or files on that computer without knowledge or consent of the human recipient.

ICT Resources

All of the University's Information and Communication Technology Resources and facilities including, but not limited to: mail, telephones, mobile phones, voice mail, SMS, facsimile machines, email, USydNet, MyUni, UniKey, eStaff, the intranet, e-Services, securID, computers, printers, scanners, access labs or other facilities that the University owns, leases or uses under Licence or by agreement, any off campus computers and associated peripherals and equipment provided for the purpose of University work or associated activities, or any connection to the University's network, or use of any part of the University's network to access other networks.

User/s

All employees, including casual employees, any person enrolled in an award course of study at the University and any person registered to attend short courses, seminars or workshops in any unit of the University, including the Centre for English Teaching and the Centre for Continuing Education as well as all other persons including members of the general public, who have been granted access to, and use of, the University's ICT Resources.

A member of the public reading public University web pages from outside the University is not by virtue of that activity alone considered to be a User.

5 Procedures

- (1) The University will set up a central email scanning process to scan all messages passed through the central mail server ("mail.usyd"). Funding for establishing and maintaining this service will be provided centrally.
- (2) Departmental mail servers or individual users may use this scanning service to relay all incoming or outgoing messages through "mail.usyd" via configuration settings. The technical details will be available from Information Technology Services on request.
- (3) The email scanning procedures and rules will be as follows:
 - All email messages will be scanned.
 - Email messages verified as harmless will be processed unchanged.
 - Email messages identified as containing known viruses or malicious content will be cleaned before continuing onward transmission; empty messages that result will either be deleted, or replaced with an appropriate warning message.
 - Emails with potentially harmful content will be defanged and forwarded along, with suitable warnings and instructions for recovery of the original message. This will include all messages not classified and handled above; eg malicious constructs in,

- Multipurpose Internet Mail Extension (MIME),
- Hypertext Markup Language (HTML)
- Extensible Markup Language (XML)
- class identifier (CLSID) or executable objects,

and other content designed to exploit vulnerabilities in email clients.

- The warnings and instructions on how to recover an original message will be designed to allow the recipient to independently verify the legitimacy of the message.
- (4) Because sender addresses can be forged by an email virus, the scanning process will never send anything back to a sender, unless the sender can be conclusively identified.
- (5) Although Departments may implement their own scanning procedures for departmental mail servers, departmental scans must be consistent with the requirements of this policy, and be as thorough as the scans on “mail.usyd”. Establishment and maintenance of such scanners should be funded by the Departments themselves.

6 Authority and consultation

(1) Development/consultation

This Policy was developed by the members of the Anti-Virus and Security Working Party of the Federation of IT Providers in consultation with staff of Faculties and the ITS .

(2) Responsibility for policy implementation, communication, monitoring and review

The Director, ITS has the overall responsibility for management of this policy.

(3) Contact

For inquiries relating to this policy, please contact the Network Security Officer, ITS:

ph: 9351 5504 fax: 9351 5001
email: security@isu.usyd.edu.au.

7 Approval

By

Chief Information Officer

01/05/04

Date of Effect

01/05/04

Proposed Date of Review

12 months from date of approval

8 References

University Policies and Guidelines

Central Email Policy and Procedures

http://www.usyd.edu.au/itc/email_procedures_june02.htm

Code of Conduct for Content Providers: http://helpdesk.usyd.edu.au/forms/C_Conduct.pdf

Freedom of Information Policy: <http://policy.rms.usyd.edu.au/000004q.pdf>

Privacy Policy: <http://www.usyd.edu.au/su/arms/privacy/policy.htm>

Privacy Management Plan: <http://www.usyd.edu.au/arms/pdf/pmp.pdf>

Policy on the Use of University Information and Communications Technology

Resources (ICT Resources) : <http://www.usyd.edu.au/ICTRPolicy>