



THE UNIVERSITY OF
NEW SOUTH WALES

UNSW Email Server Policy

<i>Policy Name:</i>	UNSW Email Server Policy	<i>Contact Officer:</i>	Jenny Beatson, Policy Officer, UNSW IT Services
<i>Approving Authority:</i>	Chief Information Officer	<i>Date of Approval:</i>	February 24 2006
<i>Due for Review:</i>	February 2008	<i>Last Amended:</i>	n/a (new policy)

UNSW recognises that policies, rules, guidelines and administrative material placed into the public domain of the University's website may be of assistance to other organisations and universities as reference material or models. The University requests that when UNSW material is used in development of documents, the work done by the University is acknowledged by referencing the source of the ideas or written expression. For further information contact Debbie Gibson, Head of Policy Management at d.gibson@unsw.edu.au

|

This policy was developed by James Dawson and Jenny Beatson, UNSW IT Services, and a working party consisting of the following members:

- Geoff Oakley, CSE
- Michael Rourke, ITS
- Ben Low, ITS
- John Warburton, ITS
- Graham Hannah, FBE
- Dawesh Chand, Law
- Shawn Sijnstra, FCE
- Tom Sedgewick, Science
- Hasitha Buckman, NSG
- Jim Leeper, Medicine
- Nigel Kersten, COFA
- Stephen Metheringham/Tony Ablong, ADFA
- Greg Fallon, FASS
- Robert Morrell, UNSW Student Services

It was then submitted for review and endorsement by the Academic Services Committee of the Academic Board (February 14 2006)

The policy was approved by Chief Information Officer Tim Cope on February 24, 2006

The policy will come into effect from April 2006

For information and assistance contact:

- IT Policy and Compliance Officer Extension 52885

There are NO previous versions of this policy.

Throughout this document, the terms "mail" and "email" are used interchangeably and have the same meaning.

Version Control

Version	Date	Author	Comment
0.1	17 March 05	J Beatson/ J Dawson	First draft
0.2	20 April 05	J Beatson	After review, J Dawson. Add policy statements
0.3	25 July 05	J Beatson J Dawson	Incorporate feedback from 22 July meeting
0.4	2 August 05	J Beatson J Dawson	Final draft for distribution prior to 2 nd meeting on 2 nd September
0.5	13 th September 05	J Beatson J Dawson B Low	Incorporate feedback from meeting 2 Sept 05
0.6	28 th September 05	J Beatson J Dawson B Low	Final revisions prior to publishing document to working party
0.7	November 05	J. Beatson	Final revision for working party – now agreed
0.8	February 06	J. Beatson	Reflect small typographical and grammatical changes requested by Academic Service Ctee.
1.0	February 06	J Beatson	Final after CIO approval

Table of Contents

1	TERMINOLOGY AND DEFINITIONS	4
2	INTRODUCTION.....	6
3	APPLICABILITY AND SCOPE.....	7
4	PRINCIPLES	7
4.1	MAIL ROUTING	7
4.2	AUTHORISATION AND COMPLIANCE	8
4.3	SENDER AND CONTENT VERIFICATION.....	8
4.4	COMMON DIRECTORY/ADDRESS BOOK.....	8
4.5	LEGISLATIVE COMPLIANCE	9
5	POLICY STATEMENTS.....	10
5.1	MAIL ROUTING	10
5.2	AUTHORISATION AND COMPLIANCE	10
5.3	SENDER IDENTIFICATION	11
5.4	COMMON DIRECTORY/ADDRESS BOOK.....	11
5.5	LEGISLATIVE COMPLIANCE	12
6	COMPLIANCE.....	13
7	DOCUMENTS REFERENCED IN THIS POLICY.....	13

1 Terminology and Definitions

GENERAL TERMS	
Address Book	An address book or a name and address book (NAB) is a book or a collection of data storing contact details (for example: address, telephone number, e-mail address, fax number, mobile phone number).
Authorised Mail Hub	Mail hubs authorised by IT Services to be permitted to connect to the Internet and other authorised mail systems. These hubs are compliant with this policy.
Authorised Mail Servers	Mail servers that comply with this policy and referenced standards and are authorised by IT Services to be permitted to connect to the Internet via approved mail hubs and other authorised mail systems.
'Bogus' email	An email with a false 'from' address, making it look as if it was sent by someone other than the real sender. These emails may contain false or misleading information; computer viruses or malicious code.
CIO	Chief Information Officer
Computer virus	Malicious code, most commonly contained in an email attachment or web link within an email. Should a recipient activate the malicious code by opening the attachment or following the web link, their computer can be seriously damaged or compromised.
CRIM Project	Central Records and Information Management Project A project to manage information with several outcomes, one of which is to ensure the UNSW manages legislative compliance with the State Records Act, to an acceptable level of risk.
Directory	The database that holds the information about objects that is to be managed by the directory service. The directory service is the interface to the directory and provides access to the data that is contained in that directory. It acts as a central authority that can securely authenticate resources and manage identities and relationships between them.
Directory Service	A directory service is a software application, or set of applications, which stores and organises information about a network and its resources -- such as users, files, printers, servers, and applications -- and allows administrators to manage access to these resources. It also provides transparency in regard to the location of these resources so users can make use of them without having to be concerned with the structure of the network.

'Phishing' Emails	Emails purporting to be from a financial institution or similar, requesting the receiver to confirm their account details, usually by logging into a fake website. If the receiver provides this information, the sender may use it to access the receiver's funds illegally.
SPAM email	Bulk mailouts of unsolicited advertising material, including links to pornographic websites.
UNSW IT Services	The central Information Technology Services group at the University of New South Wales.
TECHNICAL TERMS	
Email System	Any workable combinations of MTAs or MTAs and MUAs
Mail Hub	The term Mail Hub is used to denote an MTA or system of MTAs used to route email but not act as a mail server (having no end-user email store) since there is no MUA access. Examples could include dedicated anti-SPAM appliances, anti-virus engines running on dedicated hardware, email gateways and so forth.
Mail Server	The term Mail Server is used to denote an MTA or system of MTAs used to route email and act as a mail server, by storing email and supporting client access (MUA) using POP, IMAP or other protocols (RPC)
Mail Store	An MTA may also act as a mail store, holding the received email waiting for an MUA to access via IMAP or POP protocols
MTA	A mail transfer agent or MTA is a computer program or software agent which transfers electronic mail messages from one computer to another.
MUA	An email client (or mail user agent [MUA]) is a computer program that is used to read and send e-mail. Protocols supported by email clients include POP3 and IMAP4 and some proprietary systems use RPC (described below)
POP, IMAP, RPC	The set of protocols used to access or download email stored on an email server so it can be read on the email client. Server and client are defined below. POP – Post Office Protocol IMAP – Internet Mail Access Protocol IMAP4 – latest version, version 4 RPC – Remote Procedure Call is the protocol used by proprietary email servers such as MS Exchange and Lotus Domino/Notes to provide higher functionality access to the email server.
SMTP	Simple Mail Transfer Protocol (SMTP) is the de facto standard for email transmission across the Internet. SMTP is a simple, text-based protocol, where one or more recipients of a message are specified (and in most cases verified to exist) and then the message text is transferred. SMTP generally uses TCP port 25.

2 Introduction

Due to the devolved nature of the University, there are a number of independent email servers in operation across the campus as well as the central University email system (UniMail).

In 2004, a sharp increase in SPAM email, a proliferation of email viruses and incidents of 'bogus' emails within the University's email systems prompted the Academic Board to request that UNSW IT Services investigate ways of reducing or eradicating these threats. The central email server was blacklisted for 48 hours twice during 2004 when a server on campus was compromised, causing it to generate SPAM. These incidents highlight our responsibility to limit SPAM both ***entering*** and ***leaving*** the University's network. Accordingly, incoming and outgoing mail are separate issues that may require individual or joint solutions; however, both are within the scope of this policy.

A detailed review of the numerous email servers, including the central facility, was then undertaken by ITS, which revealed that the University currently has multiple mail server entry-points and a heterogeneous email environment, where a number of server and client email technologies co-exist. In the absence of any previous policy or authorisation requirements for mail servers, it was possible for almost any server on campus to be configured as an email server. Without appropriate security controls, these mail servers could compromise the entire University network through external attack; could allow unauthorised usage of University email facilities and could incur additional costs due to increased network traffic and excessive storage requirements. The multiple entry points increase the difficulty of tracing an email should UNSW be required to produce email as evidence and also to ensure compliance with NSW State Records Act and forthcoming CRIM requirements.

These issues highlight the University's current level of exposure to internal and external email attack. Additionally, the emerging State and Federal legislation around privacy, security and retention of data requires clear processes in order to be able to satisfy our legal and social obligations, ensuring that the University is not unduly exposed to risk and complies with legislative requirements. As the net effectiveness of any measures used against email security threats is only as effective as the weakest security link into or within the network; the review outcomes were then discussed in consultative workshops with senior Faculty and Unit stakeholders and IT managers. This has led to their subsequent in-principle agreement to the principles and policy statements in this document.

It is accepted that this policy is the first step in an ongoing process. Implementation of the policy and the development of further standards and guidelines will occur in

consultation with working parties comprising senior members of the IT community across campus. An initial standard is currently being developed.

It is further accepted that compliance with the above for some email servers may require substantial remediation, and that this will not be without cost. However, the benefits realised through improved 'bulk-buy' capacity for applications which may be shared across the campus may reduce overall costs and enhance the capability for cross-campus and cross-discipline collaboration.

3 Applicability and Scope

Through common usage, this policy is designated "Email Server Policy" and applies to all providers of email systems including email servers and email hubs at UNSW. The scope of this policy is applicable to any system connected to the UNSW Network.

4 Principles

4.1 Mail Routing

All ***external*** UNSW Email (Incoming, Outgoing) ***shall*** only route through Authorised Mail Hubs.

All ***internal*** UNSW Email (server to server) ***should*** route through Authorised Mail Hubs.

Rationale:

To reduce computer virus infections on campus, stop inappropriate email relaying and to provide a consistent approach to management of SPAM and virus email, all UNSW incoming and outgoing email will be routed via authorised mail hubs to ensure all email is adequately scanned. Central routing of mail will greatly enhance and simplify the logging and audit of emails for production of evidence and potential records compliance requirements.

Implications:

Administrators of authorised mail systems will be responsible for maintaining effective virus and SPAM scanning processes, and shall also store appropriate meta-data for records compliance purposes. Mail servers shall route all incoming and outgoing email via an authorised mail hub for scanning. Only authorised hubs will be able to communicate off campus using SMTP. Any email ***not*** routed centrally will require the administrator to keep audit logs which shall be provided to IT Services on request.

4.2 Authorisation and Compliance

All Email Systems shall be approved by CIO (or delegate) and comply with UNSW standards.

Rationale:

Email systems external to the central ITS facility may be set up, but because email is a core service and interacts with so many other functions, any new installation shall be authorised by the Chief Information Officer (CIO) (or delegate), and conform to a minimum set of operating standards, and to a set of standard interfaces and protocols.

Implications:

All email systems (including central ITS facilities) shall conform to a minimum set of operating standards and to a set of standard interfaces and protocols. They shall also be recorded in a central inventory held by ITS. Applications for new email systems shall be approved by the CIO or delegate on submission of a business case explaining why a new server is required.

The sets of operating standards, interfaces and protocols will be developed in collaboration with the relevant Faculties and Units.

4.3 Sender and content verification

The content and sender of an email should be verifiable.

Rationale:

Because instructions may be followed or actions taken based on official UNSW email, the authenticity of the content and the identity of the sender shall be assured with an acceptable level of confidence.

Implications:

All email systems shall be compatible with UNSW email identity standards.

4.4 Common Directory/Address Book

All address books housed on email servers shall be protected and shall contain correct identification and email address information.

Rationale:

The establishment of a full common UNSW address directory will enhance collaboration and efficiency through the ability to locate correctly intended email recipients from within an email system, reduce delivery errors and comply with privacy standards.

Implications:

Email systems will be required to support common and/or open standards to facilitate communication and interoperability of address book data. All email systems shall be configured to comply with UNSW directory standards.

4.5 Legislative Compliance

All email systems will comply with appropriate legislation.

Rationale:

Recent tightening of Federal, State and other legislation around privacy, security and retention of data requires a clear email server policy in order to be able to satisfy our legal and social obligations, ensuring that the University is not unduly exposed to risk and complies with legislative requirements.

Implications:

By requiring all email servers to adhere to the above principles, UNSW will enhance its legislative compliance capability and reduce the risk of adversarial litigation.

5 Policy Statements

5.1 Mail Routing

All **external** UNSW Email (Incoming, Outgoing) **shall** only route through Authorised Mail Hubs.

All **internal** UNSW Email (server to server) **should** route through Authorised Mail Hubs.

<i>Relates to Principle(s)</i>	<i>4.1 Authorised Mail Hubs</i>
<i>Accompanying Standard/Guideline</i>	<i>"UNSW Mail Server Standard" – to be developed</i>

Email is a key communication medium for the University and as such, shall be protected from such threats as computer viruses, malicious code, bogus emails, SPAM, phishing emails and denial of service attacks.

All UNSW incoming and outgoing email **shall** be routed via authorised mail hubs for scanning. Only these authorised hubs will be able to communicate off campus. All internal mail **should** be routed via authorised mail hubs.

Administrators of authorised mail systems will be required to maintain effective virus and SPAM scanning to a level meeting or exceeding that defined in the UNSW Mail Server Standard.

5.2 Authorisation and compliance

All Email Systems shall be approved by the CIO (or delegate) and comply with UNSW standards.

<i>Relates to Principle(s)</i>	<i>4.2 Authorisation and Compliance with Standard</i>
<i>Accompanying Standard/Guideline</i>	<i>"UNSW Mail Server Standard" – to be developed</i>

All existing UNSW email systems shall be recorded in a central inventory, to be held in ITS. Additional email servers external to the central facility may be set up, but shall be authorised by the CIO or delegate on submission of a business case approved by the Dean, Head of School or business unit, explaining why a new server is required.

The UNSW Mail Server Standard will be developed in consultation with senior Faculty and Unit IT managers. Once developed, all email servers will be required to comply with these standards.

5.3 Sender Identification

The content and sender of an email should be verifiable.

<i>Relates to Principle(s)</i>	4.3 Content and Sender Verification
<i>Accompanying Standard/Guideline</i>	"Standard Identity Mechanism" – to be developed

As instructions may be followed or actions taken based on official UNSW email, the authenticity of the content and the identity of the sender and receivers must be able to be assured.

A common standard identity mechanism will be developed in consultation with senior Faculty and Unit IT managers. Once developed, it should be followed by all email servers in order to provide this assurance.

Some Faculties, Schools and Business Units may use standard email disclaimers for branding or duty-of-care purposes. Ideally, these should be stored on the server and automatically added to outgoing emails, rather than individual users having to configure them as part of their signature.

5.4 Common Directory/Address Book

All address books housed on email servers shall be protected and shall contain correct identification and email address information.

<i>Relates to Principle(s)</i>	4.4 Common Directory/Address Book
<i>Accompanying Standard/Guideline</i>	"UNSW Mail Server Standard" – to be developed

At present, with the variety of mail servers and email applications in use across campus, it is not possible to provide a full common email address directory for UNSW. This hampers efficiency and collaboration, and contributes to delivery errors. The lack of a University-wide directory service has also forced many groups to develop their own directories, which may contain:

- Insufficient security or privacy mechanisms to ensure email addresses cannot be 'harvested' by SPAMmers and;
- Public display of specific staff location information (eg Room 123). In some cases it may be necessary to keep this level of information private to ensure the personal safety of students and staff.

It is recommended that the UNSW Mail Server Standard document to be developed (see 5.2) includes the requirement that email servers support common and/or open standards which facilitate synchronisation of address book data.

5.5 Legislative Compliance

All email systems will comply with appropriate legislation

<i>Relates to Principle(s)</i>	<i>4.5 Legislative Compliance and Fiscal Prudence</i>
<i>Accompanying Standard/Guideline</i>	<i>"UNSW Mail Server Standard" – to be developed</i>

The University has legal and moral obligations to comply with relevant State and Federal legislation, as well as the requirements of its own internal policies.

Users of email facilities are required to comply with the "UNSW Email Policy", which focuses on appropriate 'behavioural' use of email. However, administrators of email servers are not exempt from ensuring that the University is not unduly exposed to risk, and that its email facilities comply with legislative requirements, particularly those relating to privacy, security and retention of data.

This policy extends the UNSW email policy beyond UNIMAIL to include reasonable use of ALL approved email systems.

Privacy and confidentiality shall be protected by having strong and secure authentication and storage processes. UNSW business-related email shall be stored for varying periods of time in compliance with the State Records Act, and so as to be able to retrieve emails if so directed by authorised bodies.

Appropriate audit logs of email shall therefore be kept and backed up as the first step to identify and retrieve emails for the purpose of providing evidence or record.

6 Compliance

Penalties for non-compliance are to be further agreed with working group, but will include the option of shutting down unauthorised mail servers without notice and; enforced use of central mail facilities in the case of repeat breaches.

It should be noted that email servers found to be configured (intentionally or unintentionally to act as open relay or open proxy servers will be shut down without notice.

7 Documents Referenced in this Policy

- **Rules Relating to the Use of Computing and Electronic Communication Facilities at the University of New South Wales,**
<http://www.infonet.unsw.edu.au/poldoc/rulcomp.htm>
- **UNSW Code of Conduct,**
<http://www.hr.unsw.edu.au/poldoc/codecond.htm>
- **Privacy and Personal Information Protection Act 1998 (NSW),**
http://www.austlii.edu.au/au/legis/nsw/consol_act/papipa1998464/index.html
- **State Records Act 1998 (NSW)**
<http://www.records.nsw.gov.au/about/act.htm>
- **Privacy Act 1988 (Commonwealth),**
<http://scaleplus.law.gov.au/html/pasteact/0/157/top.htm>
- **UNSW Privacy Management Plan,**
<http://www.privacy.unsw.edu.au/pmp.htm>
- **Student Misconduct Rules,**
<http://www.infonet.unsw.edu.au/poldoc/stumis.htm>
- **UNSW Electronic Record-Keeping Policy**
http://www.infonet.unsw.edu.au/ras/policy/electronic_recordkeeping.htm
- **UNSW Record-Keeping Policy**
<http://www.infonet.unsw.edu.au/ras/policy/recordkeeping.htm>
- **UNSW IT Security Policy**
http://www.its.unsw.edu.au/policies/pol_security.html

- ***UNSW Email Policy***
http://www.its.unsw.edu.au/policies/docs/Email_Policy_2004.pdf