Information Security Policy

Aligarh Muslim University

Aligarh

Document History and its version

Information Security Policy
Aligarh Muslim University
Aligarh
Current Version : 1.0
Proposed by : Director, Computer Centre

Date	Version	Revision Class	Remark
19-Aug-2014	✓ Initial Draft	N.A.	Put up for review by Vice Chancellor. Vice Chancellor approved the same, with comments for minor revision.
02-Sep-2014	✓ 1.0	Minor	Comments of the Vice Chancellor on the Information Security Policy is incorporated.

Aligarh Muslim University, Aligarh

Computer Centre

Information Security Policy

1. Objective

This policy provides a framework for the management of information security throughout the Aligarh Muslim University (referred as “University). It applies to:

1.1 all those with access to University information systems, including staff, students, visitors, guests and contractors;

1.2 any systems attached to the University computer or internet network or telephone networks and any systems supplied by the University or used in the University;

1.3 all information (data) processed by the University pursuant to its operational activities, regardless of whether it is processed electronically or in paper (hard copy) form, any communications sent to or from the University and any University information (data) held on systems external to the University’s network;

1.4 all external parties that provide services to the University in respect of information processing facilities and business activities; and

1.5 principal information assets including the physical locations from which the University operates.

2. Aims and Commitments

2.1 The University recognises the role of information security in ensuring that users have access to the information they require in order to carry out their work. Computer and information systems underpin all the University’s activities, and are essential to its research, teaching and administrative functions.

2.2 Any reduction in the confidentiality, integrity, or availability of information could prevent the University from functioning effectively and efficiently. In addition, the loss or unauthorised disclosure of information has the potential to damage the University’s reputation and cause financial loss. The University has the power to impose suitable fine on organisations for breaches of the provisions of Information Security Policy (referred as ISP).

2.3. To mitigate these risks, information security must be an integral part of information management, whether the information is held in electronic or hard copy form.

2.4. The University is committed to protecting the security of its information and information systems in order to ensure that:

2.4.1 the integrity of information is maintained, so that it is accurate, up to date and ‘fit for purpose’;

2.4.2 information is always available to those who need it and there is no disruption to the business of the University;

2.4.3 In order to meet these aims, the University is committed to implementing security controls that conform to best practice, as set out by the rules prescribed from time to time.

2.4.4 An information and communication technology policy regulator, comprising representatives from all relevant parts of the University, shall advise on best practice and coordinate the implementation of information security controls (please refer to sections 3.2 for further information).

2.4.5 The University will establish and maintain appropriate contacts with other organisations, law enforcement authorities, regulatory bodies, and network and telecommunications operators in respect of its information security policy.

2.4.6 Breaches of information security must be recorded and reported to appropriate bodies in the University, who will take action and inform the relevant authorities (please refer to sections 6.13 and 9 for further information).

2.4.7 This Policy and all other supporting policy documents shall be communicated as necessary throughout the University to meet its objectives and requirements.

3. Responsibilities

3.1 **Executive Council** (referred as EC) has ultimate responsibility for information security within the University. More specifically, it is responsible for ensuring that the University complies with relevant external requirements, including legislation.

3.2 The **Policy Regulator on Information and Communication Technology(PRICT)** (refer sec 2.6)constituted by the EC and the relevant ordinances shall be the principal policy regulator constituted under the chairmanship of Vice-Chancellor and Director Computer Centreas Convener shall be responsible to EC for:

3.2.1 ensuring that users are aware of this policy;

3.2.2 seeking adequate resources for its implementation;

3.2.3 monitoring compliance;

3.2.4 conducting regular reviews of the policy, having regard to any relevant changes in legislation, organisational policies and contractual obligations; and

3.2.5 ensuring there is clear direction and visible management support for security initiatives.

3.3 Head of department/centre/unit/office

3.3.1 Given the University’s devolved structure, all Officers of the University/ Deans/ Controller/ DSW/ Proctor/ Chairman/ Principals/ Directors/ other heads (referred as heads) are responsible for information security within their office/departments/units (referred as department). They may ensure that the department has in place a local information security policy if required with the approval of the PRICT to meet its own particular needs, consistent with the requirements of this overarching policy. The local information security policy should identify the department's own information security requirements and provide a management framework for meeting those requirements. 'Department' in this context includes all equivalent local units as described above.

3.3.2 Specific roles and responsibilities for information security within departments should be clearly identified subject to acceptance by PRICT.

3.3.3 The head of department must propose the policy to the PRICT for approval, and ensure that it is implemented and kept under regular review.

3.4 Users and External Parties

3.4.1 Users of University information will be made aware of their own individual responsibilities for complying with University and departmental policies on information security.

3.4.2 Agreements with third parties involving accessing, processing, communicating or managing the University's information, or information systems, should cover all relevant security requirements, and be covered in contractual arrangements.

3.4.3All login IDs and passwords related to departments shall be under the control of the head and shall be transferred to the incumbent with the transfer of charge whenever occur.

3.4.4 The management of display content including websites contents, updates, inclusions, and deletions shall also be the responsibility of the head.

4. Data Protection

4.1 Personal and official data must be handled in accordance with the University's policy and guidance on personal data under the Indian Constitution ("Constitution") and the Information Technology Act, 2000, the Indian Contract Act, 1872, the Copyright Act, 1957, RTI, 2005 and the Indian Penal Code, 1860, protect property rights.

4.2 The University requires that appropriate technical and organisational measures are taken against unauthorised or unlawful processing of data and against accidental loss or destruction of, or damage to, data.

4.3 A higher level of security should be provided for 'sensitive data', which is definedby the University as data relating to ethnic or racial or communal origin, religious beliefs, physical or mental health, sexual life, political opinions, trade union membership, or the commission or alleged commission of criminal offences.

5.Protection of Information Systems and Assets

5.1 Concurrent to the University ISP the departments may draw up their own information security policy, setting out appropriate controls and procedures, in accordance with the University rules. Information owners must be satisfied that the controls will reduce any residual risk to an acceptable level, in line with the practices outlined by the University

5.2. Confidential information should be handled in accordance with the requirements set out in section 6 below.

6. Protection of Confidential Information

Identifying confidential information is a matter for assessment in each individual case. Broadly, however, information will be confidential if it is of limited public availability; is confidential in its very nature; has been provided on the understanding that it is confidential; and/or its loss or unauthorised disclosure could have one or more of the following consequences:

i. financial loss*e.g. the withdrawal of a research grant or donation, a fine by the EC and/or funding agency, a legal claim for breach of confidence;*
ii. reputational damage*e.g. adverse publicity, demonstrations, complaints about breaches of privacy; and/or*
iii. an adverse effect on the safety or well-being of members of the University or those associated with it*e.g. increased threats to staff or students engaged in sensitive research, embarrassment or damage to benefactors, suppliers, staff and students.*

6.1 Storage

6.1.1Confidential information should be kept secure, using, where practicable, dedicated storage (e.g. file servers) rather than local hard disks, and an appropriate level of physical security.

6.1.2. File or disk encryption should be considered as an additional layer of defence, where physical security is considered insufficient.

6.2Access

6.2.1 Confidential information must be stored in such a way as to ensure that only authorised persons can access it.

6.2.2 All users must be authenticated. Authentication should be appropriate, and where passwords are used, clearly defined policies should be in place and implemented. Users must follow good security practices in the selection and use of passwords.

6.2.3 Where necessary, additional forms of authentication should be considered.

6.2.4 To allow for potential investigations, access records should be kept for a minimum of six months, or for longer, where considered appropriate.

6.2.5 Users with access to confidential information should be security vetted, as appropriate, in accordance with existing policies.

6.2.6 Physical access should be monitored, and access records maintained.

6.3 Remote access

6.3.1 Where remote access is required, this must be controlled via a well-defined access control policy and tight access controls provided to allow the minimum access necessary.

6.3.2 Any remote access must be controlled by secure access control protocols using appropriate levels of encryption and authentication.

6.4 Copying

6.4.2 The number of copies made of confidential information, whether on portable devices or media or in hard copy, should be the minimum required, and, where necessary, a record kept of their distribution. When no longer needed, the copy should be deleted or, in the case of hard copies, destroyed (see 6.12.5).

6.4.3 All copies should be physically secured e.g. stored in a locked cupboard drawer or filing cabinet.

6.5 Disposal

Policies and procedures must be in place for the secure disposal/destruction of confidential information

6.6 Use of portable devices or media

6.6.1 Procedures should be in place for the management of removable media in order to ensure that they are appropriately protected from unauthorised access.

6.6.2 The permission of the information owner should be sought before confidential information is taken off site. The owner must be satisfied that the removal is necessary and that appropriate safeguards are in place e.g. encryption.

6.6.3 In the case of personal data, the ICO recommends that all portable devices and media should be encrypted where the loss of the data could cause damage or distress to individuals.

6.6.4 The passphrase of an encrypted device must not be stored with the device (see also section 6.8.2).

6.7 Exchange of Information and use of Email

6.7.1 Controls should be implemented to ensure that electronic messaging is suitably protected.

6.7.2 Email should be appropriately protected from unauthorised use and access.

6.7.3 Email should only be used to send confidential information where the recipient is trusted, the information owner has given their permission, and appropriate safeguards have been taken e.g. encryption.Provided further that the risks associated with the use of e-mail shall be taken into consideration.

6.8 Cryptographic controls

6.8.1 Procedures should be in place to support the use of cryptographic techniques and to ensure that only authorised personnel may gain access to confidential information.

6.8.2 University guidance, on cryptographic policy and key management, should be followed to ensure that data are appropriately secured and that all legal and regulatory requirements have been considered.

6.9 System planning and acceptance

A risk assessment should be carried out as part of the business case for any new ICT system that may be used to store confidential information. The risk assessment should be repeated periodically on any existing systems.

6.10 Backup

Information owners should ensure that appropriate backup and system recovery procedures are in place. Backup copies of all important information assets should be taken and tested regularly in accordance with such an appropriate backup policy.

6.12 Hard Copies

Protective marking

6.12.1 Documents containing confidential information should be marked as ‘Confidential’ or with another appropriate designation e.g. ‘sensitive’, etc, depending on the classification system adopted by the department.

Storage

6.12.2 (a) Wherever practicable, documents with confidential information should be stored in locked cupboards, drawers or cabinets. Where this is not practicable, and the information is kept on open shelving, the room should be locked when unoccupied for any significant length of time.

(b) Keys to cupboards, drawers or cabinets should not be left on open display when the room is unoccupied.

Removal

6.12.3 Confidential information should not be removed from the University unless it can be returned on the same day or stored securely overnight, as described in section 6.12.2 above.

Transmission

6.12.4 (a) If confidential documents are sent by fax, the sender should ensure they use the correct number and that the recipient is near to the machine at the other end ready to collect the information immediately it is printed.

(b) If confidential documents are sent by external post, they should ideally be sent by a form of recorded delivery. The sender must ensure that the envelope is properly secured.

(c) If confidential documents are sent by internal post the documents should be placed in an envelope marked ‘Confidential’ with the addressee’s name clearly written on it.

Disposal

6.12.5. Confidential documents must be shredded in a confidential manner prior to disposal.

6.13Enforcement

6.13.1 There must be a written policy in place at the local level for the handling of confidential information, whether electronic or hard copy and a copy of the procedures must be provided to every user so that they are aware of their responsibilities.

6.13.2 Any failure to comply with the policy may result in disciplinary action.

6.13.3 Any loss or unauthorised disclosure must be promptly reported to the owner of the information.

6.13.4 Computer security incidents involving the loss or unauthorised disclosure of confidential information held in electronic form must be reported to Director, Computer Centre at it.security@amu.ac.in- and investigated.

6.13.5 If the loss or unauthorised disclosure involves personal data, whether electronic or hard copy, the University’s Registrar must also be informed.

7. Information Display Policy

7.1 The Policy on Information Display shall be regulated by the Web Committee constituted by the Vice-Chancellor and the relevant rules shall be framedby the EC and shall be responsible to EC for:

7.1.1 dissemination of information

7.1.2 ensuring awareness of the users;

7.1.3 seeking adequate resources for its implementation;

7.1.4 monitoring compliance;

7.1.5 conducting regular reviews of the policy, having regard to any relevant changes in legislation, organisational policies and contractual obligations; and

7.1.6 ensuring there is clear direction and visible management support for security initiatives.

7.2 AMU Campus users interested in altering / putting specific items of information on display under various categories on the AMU, Aligarh home page (www.amu.ac.in) or on pages under control of Web Committee/Director, Computer Centre/Webmaster may note the following:

7.2.1. All mails requesting such changes need be addressed to: webmaster@amu.ac.in

7.2.2. All such requests may be sent using an 'amu' mail account. No requests from personal accounts would be processed.

7.2.3. Students making such requests may route them through concerned faculty or by copying the mail to the faculty.

7.2.4. An information item requested for display on the home page need be of the nature of a "News" or "Event" of reasonable import. However, the final discretion for accepting such a request would be with the of Web Committee/Director, Computer Centre/Webmaster.

7.2.5. All communication relating to display on the home page need to provide a concise title (normally not exceeding 30 characters) of the item and also indicate the time period of the display, after which it may be removed.

7.2.6. In case a file has to be hosted as part of the information item, users may use html or pdf formats only.

7.2.7. For posting information relating to R&D, awards, honours, achievements etc, the user (s) need to send an authoritative text along with suitable photographs (if available). Only texts authored (or dictated) by AMU faculty / student (or a concerned administrative office) would be accepted. The text may be composed in a very brief "abstract" form for a general readership. Substitute reports on the same topic prepared by external agencies (or links owned by such agencies) will not be accepted for direct hosting on the institute main page / site. This is for ensuring authenticity, and for avoidance of possible (even if, inadvertent) oversights / errors / misrepresentation in reportage by such agencies.

7.2.8. External users may note that the webmaster may be contacted only for situations pertaining to any malfunction of the links on the AMU, Aligarh website. The webmaster does not process mails pertaining to institute administration matters.

8. Compliance

8.1 The University has established this policy to promote information security and compliance with relevant legislation. The University regards any breach of information security requirements as a serious matter, which may result in disciplinary action.

8.2 Compliance with this policy should form part of any contract withstaff, students, visitors, guests, contractors,and any third party that may involve access to network or computer systems or data as per Declaration - Statement of Policy

Undertaking with respect to AMU, Aligarh IT Usage Policy

All users of AMU, Aligarh will be subject to the following **Acceptable Use Policy**

8.2.1. [Content] I shall be responsible for all use of this network. In case I own a computer and decide to connect it to AMU, Aligarh network, I will be responsible for all the content on it, especially that which I make available to other users. (This provision will also apply to any computer or device for which I am responsible, and is included in the meaning of “my computer”.) In case I do not own a computer but am provided some IT resources by AMU, Aligarh, I will be held responsible for the content stored in the designated workspace allotted to me (examples: file storage area, web pages, stored/archived emails, on Computer Centre or Department machines). I will also be responsible for the use of unlicensed softwares and applications.

8.2.2.[Network]I will be held responsible for all the network traffic generated by “my computer”. I understand that network capacity is a limited, shared resource. I agree that physically tampering with network connections/equipments, sending disruptive signals, or making EXCESSIVE USE of network resources is strictly prohibited. Repeated offenses of this type could result in permanent disconnection of network services. I shall not share the network connection beyond my own use and will not act as a forwarder/ masquerader for anyone else.

8.2.3.[Academic Use]I understand that the IT infrastructure at AMU, Aligarh is for academic use and I shall not use it for any commercial purpose or to host data services for other people or groups. Also, I shall not host or broadcast information that might harm others or may be otherwise considered objectionable or illegal as per Indian law. I shall not indulge in disrespecting religious beliefs, physical or mental health, sexual life, political opinions, trade union membership, or the commission or alleged commission of criminal offences.

8.2.4.[Identity]I shall not attempt to deceive others about my identity in electronic communications or network traffic. I will also not use AMU, Aligarh IT resources to threaten, intimidate, or harass others.

7.2.5.[Privacy]I will not intrude on privacy of anyone. In particular I will not try to access computers (hacking), accounts, files, or information belonging to others without their knowledge and explicit consent.

I shall pass on the IT resources passwords and related information to the incumbent at the time of transfer of charge required under official capacity or surrenders the account and password at the termination of services or tenure or studentship.

8.2.6.[Monitoring]I understand that the IT resources provided to me are subject to monitoring, with cause, as determined through consultation with the AMU, Aligarh administration, when applicable. The monitoring may include aggregate bandwidth usage to effectively manage limited IT resources as well as monitoring traffic content in response to a legal or law enforcement request to do so. I authorize AMU, Aligarh administration to perform network vulnerability and port scans on my systems, as needed, for protecting the overall integrity and efficiency of AMU, Aligarh network.

8.2.7.[Viruses]I shall maintain my computer on this network with current virus detection software and current updates of my operating system, and I shall attempt to keep my computer free from viruses, worms, trojans, and other similar programs.

8.2.8.[File Sharing]I shall not use the IT infrastructure to engage in any form of illegal file sharing (examples: copyrighted material, obscene material). In particular, I have noted the following:

Electronic resources such as e-journals, e-books, databases, etc. made available by the Maulana Azad Central Library and other libraries of AMU, Aligarh are for academic use. These resources can be searched, browsed, and material may be downloaded and printed as single copies of articles as is done in the case of printed library material. Downloading or printing of a complete book or an entire issue or a volume of one or more journals (called systematic downloading) is strictly prohibited. Use of robots, spiders or intelligent agents to access, search and/or systematically download from the e-resources is also prohibited. Any violation of this policy will result in penal action as per the rules and regulations of the Institute. I am aware that Systematic downloading will result in the publisher blocking the entire community of users at AMU, Aligarh from accessing these resources.

8.2.9. [Security] I understand that I will not take any steps that endanger the security of the AMU, Aligarh network. Specifically, I will not attempt to bypass firewalls and access rules in place. This includes not setting up servers of any kind (examples: web, mail, proxy) that are visible to the world outside the AMU, Aligarh campus. In critical situations, AMU, Aligarh authorities reserve the right to disconnect any device or disable any account if it believed that either is involved in compromising the information security of AMU, Aligarh.

8.2.10. [Penalties] I understand that any use of IT infrastructure at AMU, Aligarh that constitutes a violation of AMU, Aligarh Regulations could result in administrative or disciplinary procedures.