SEEDA POLICY FOR

DATA SECURITY & EQUIPMENT USE

Applicable to:

- Electronic & manually held data
- Desktop & Laptop Computers
- Data Storage & Retrieval Systems
- E-mail Use
- Internet Use
- Intranet Use

July 2006

Contents

1. Introduction.

The purpose of this Policy and the guidelines associated with it is to ensure that all employees understand their responsibilities in the use of SEEDA Desktop/Laptop computer systems, E-mail, Internet and Intranet facilities and respond appropriately to the opportunities and risks occasioned by their use. The Policy applies to all staff equally and failure to comply with it will, in some circumstances, lead to disciplinary action. Please note that APPENDIX 2 of SEEDA Terms & Conditions of Employment, 'DISCIPLINARY RULES AND PROCEDURES' applies to any reference to misconduct, a breach of rules, or gross breach of rules.

2. Data Security & Access

2.1 Any unauthorised attempt to access a SEEDA system without appropriate password(s) and authority is regarded as gross breach of rules. It may also be a criminal act and lead to criminal proceedings.

2.2 Employees must take appropriate care not to disclose passwords or otherwise make them accessible by and available to unauthorised persons in any circumstances whether by electronic or other means. In the event of doubt please contact IT management for advice and instruction as failure to take appropriate steps will in some circumstances be regarded as a breach of rules.

User Guidelines

2.3 IT systems password combinations must not be easily guessed or deduced. Examples of bad passwords include, "password", "1234", "abcd", "hello" because they offer little protection against attempts at unauthorised access. Similarly, maintaining passwords by appending numbers to them is also poor practice (i.e. john1, john2, john3 etc).

2.4 Passwords should be a minimum of seven characters in length. Examples of good password practice include long passwords, mixing of character and case, and passwords that relate to uniquely personal knowledge or information not widely known to others.

2.5 Users must set a password when prompted to do so. Blank passwords are not permitted.

2.6 Passwords (except those set by a recognised system administrator) must expire after 90 days.

2.7 Passwords should contain non-alphabetic characters and capital letters, (for example, w£lc0M£ instead of welcome).

2.8 Users are not permitted to re-use any password until it has been followed by five different consecutive passwords.

2.9 A user-account will be disabled after three failed authentication attempts.

3. Data Privacy & Property Rights

3.1 Information available to and accessed by SEEDA staff in the course of their employment is likely to be private and confidential, and unauthorised disclosure of it may damage the interests of SEEDA, its partners, clients, employees and other interests. Unauthorised disclosure, whether by electronic or non-electronic means, may amount to a gross breach of rules.

3.2 All information contained within the SEEDA servers and e-mail system is the property of SEEDA. The agency reserves the right to access any user's data and/or mailbox where it is suspected that a user's activities are illegal or detrimental to the agency. The same criteria apply whereby the agency reserves the right to deny access to any user's data and/or mailbox. Such action will require the authorisation of an executive director and will be subject to regular review.

3.3 Employees must comply with the requirements of ***The Data Protection Act*** and ***The Computer Misuse Act*** and failure to do so may be regarded as a breach of rules as well as amounting to a breach of law. Electronic copies of these policies are available on SEEDA's document management system which you can access through the SEEDA Information on Demand (SID) intranet.

3.4 Staff are individually responsible for receiving, using and storing data accessible by them in an appropriate manner; preserving it with care; and returning it to a safe place of storage after use. This is particularly important where confidential and commercially sensitive data is concerned and the requirement applies to data relating to SEEDA or SEEDA's associated bodies. It applies to all document formats, electronic (e.g. email and attachments) as well as paper documents including drafts. Intentional or negligent acts or omissions that might compromise the integrity or availability of commercial data may be treated as a breach of rules.

3.5 Disclosure of any personal or private information about an individual connected with SEEDA through its activities, and without that person's permission, particularly information potentially damaging to their reputation or standing, may amount to a breach of rules. This will apply whether or not the information disclosed is true or untrue.

4. Software Licensing and Piracy

4.1 Any SEEDA staff member producing or installing or otherwise using unauthorised copies of software applications, entertainment media or any other electronic content in contravention of a manufacturer's copyright does so illegally. Such action may in some circumstances constitute a breach of rules.

User Guidelines

4.2 The installation and configuration of freeware, shareware, or any application not part of the computer's initially delivered configuration must be authorised by the IT department. The SEEDA IT department will require a business case for the application before installing it.

4.3 The IT department will cease providing support for any computer running un-authorised software until that software is removed.

4.4 All licences required for applications must be purchased, before that application is installed on any SEEDA computer.

4.5 Computers running unlicensed software will have that application removed immediately upon discovery, regardless of disruption of service.

4.6 Any SEEDA staff member, who knowingly uses unlicensed applications, will be deemed to be operating illegally. They may face severe disciplinary action and be reported to the relevant authorities. Any SEEDA staff member who is aware of any other staff member who knowingly uses unlicensed applications should report this to his line manager or Human Resources.

5. Asset Management

5.1 Users will be held accountable for the condition and safe keeping of all assets supplied by SEEDA. They are expected to maintain them as closely as possible to their issued condition and to use them for their supplied purpose and at their supplied location. Damage or loss arising through inappropriate or unauthorized use may constitute misconduct and may be regarded as a breach of rules.

User Guidelines

5.1 Any user operating IT equipment devoid of, or fitted with, a damaged or tampered asset label must report the equipment to the IT department.

5.2 The IT department must be informed of any relocation of assets purchased through the IT department.

5.3 Tampering with or modifying an asset label may be misconduct in accordance with SEEDA disciplinary rules and procedures.

5.4 Desktop computers and peripherals must not be taken from SEEDA premises without the express permission of the IT Department.

5.5 Users must sign an acceptance form for any IT asset leaving the premises. This must be carried out in the presence of an IT staff member before it leaves. IT loan equipment (such as laptops) must be returned to the IT helpdesk and the loan form should be signed off by an IT staff member.

6. Internet and E-mail Use

Terms of Internet Use

6.1 Company systems are for business use. However SEEDA accepts that employees will occasionally use the Internet and email for non-business related activities. Such activity should be occasional and, wherever possible, take place outside normal

working hours. Importantly however, access to Internet sites, containing any of the materials listed in 6.3 below is prohibited and any employee found to have accessed it using SEEDA equipment may be committing a breach of rules.

6.2 Personal use of both the Internet and email must not be excessive and must not interfere with an individual's job performance. Excessive use of email and Internet for personal use may ultimately amount to a breach of rules.

User Guidelines

Internet Restrictions

6.3 Access to the following themed Internet sites is strictly prohibited and access is therefore blocked by protective software:

- Adult material – containing adult content, nudity, sexual images
- Gambling
- Illegal/questionable legality
- Racism/hate
- Tasteless
- Violence
- Games

However as the Internet is growing so rapidly, it is impossible to prevent all inappropriate access automatically.

Downloading of Internet Material

6.4 The greatest risk from viruses lies in downloaded programmes and executable files. Spreading of viruses is subject to prosecution under *The Computer Misuse Act 1990* and all software for use in SEEDA must be obtained from controlled legal sources by the IT Department.

6.5 You should therefore not download any software without the prior permission of the IT Department. This includes software, screensavers, games and shareware available free on the Internet.

Copyright Laws

6.6 *The Copyright, Designs and Patents Act 1998* states that only the owner of the copyright is allowed to copy the information. Any copying, without permission, including electronic copying, is prohibited. These copyright laws apply not only to documents but also to software.

Email etiquette

6.7 Although email communication has the same speed and apparent informality as using the telephone, it also has the permanence of written communications

and, as such, must be controlled to ensure that it meets the same standards as other published documents.

6.8 Employees are reminded that the same laws apply to email messages as to any other written document and that therefore they should avoid making any inaccurate or defamatory statements. There is an essential need for responsibility when writing an email and if there is any doubt over its contents, you should seek advice from relevant sources (colleagues, manager or the IT team) before sending such a message. Further, employees should be aware that contracts may inadvertently make contracts on behalf of SEEDA or inadvertently vary the terms of any existing contract by e-mail. Particular care should be taken to avoid any such action.

6.9 Email messages should not include defamatory, libellous or sexually harassing statements or offensive comments based on gender, age, sexuality, race, disability or appearance. Email harassment is completely unacceptable in terms of SEEDA's commitment to its employees and offensive email messages will not be tolerated. SEEDA's Equal Opportunities and Dignity at Work Policy refers. Any communication which causes offence whether given by email or any other way including spoken may be regarded as a breach of rules or a gross breach of rules.

6.10 As a general guide to email etiquette, all individuals using SEEDA's email facility are advised to consider the following:

- Only use emails where appropriate. Whilst email is excellent for a quick comment, it is not interactive and should not be used as a substitute for face to face communication or use of the telephone;
- Only send emails to individuals when it essential that they receive that information and the information is intended for them e.g. avoid mass mailings to entire offices when the message is only relevant to a small proportion of staff;
- Do not assume that if an individual is copied in on an email, he/she is in agreement with the contents of the message;
- Do not accept that, on sending an email, the recipient has received, read or even understood the email. Check with the recipient as necessary;
- Avoid lengthy chain discussions over email, meet with the respondent face to face to openly discuss such issues and build on your working relationships;
- Do not use printed chain emails as a briefing document or source of information for other individuals;
- Never say anything in an email that you would not be prepared to say directly to the recipient concerned, or in some other formal documentation;
- Refrain from typing email messages in upper case font as the use of capital letters in emails is generally considered to represent SHOUTING;
- If a message requires a response, respond quickly and within the given timescales. Refer to SEEDA's service standards as necessary;
- Do not using the email as a tool for distributing jokes and forwarding nuisance emails;

- Do not advertise items for sale over the email system. Email is not for the personal gain of individuals. Office notice boards may be used for this purpose.

6.11 If clarification on email use and etiquette is required, you should contact a member of the HR team.

Monitoring

6.12 SEEDA respects each individual's right to privacy and respects the privacy of their correspondence.

6.13 Software exists to protect SEEDA's internal network from external threats such as virus infection, unauthorised access and/or misuse. All incoming/outgoing Internet mail is monitored and screened by such software for such purposes.

6.14 Individual email accounts are not, under normal circumstances, monitored except for size due to limits on disk space for storage. However employees should be aware that under the *Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000*, SEEDA may monitor or record employees' communications (such as email or telephone) for the following purposes:

- For recording evidence of business transactions
- Ensuring compliance with regulatory or self-regulatory guidelines
- Maintaining the effective operation of the employer's systems (e.g. preventing viruses)
- Monitoring standards of training and service
- Preventing or detecting criminal activity
- Preventing the unauthorised use of the computer/telephone system – i.e. ensuring that SEEDA's Internet and Email Policy is not breached

Employee's internet use may also be monitored for the same purposes.

Disciplinary issues

6.15 Any disciplinary action arising from inappropriate use of or access to the Internet by a SEEDA employee will be in accordance with SEEDA 'DISCIPLINARY RULES AND PROCEDURES' as notified and amended from time to time, taking account the effect of the conduct on the following:

- Employee productivity
- Disruption to the SEEDA network
- Creation of a hostile working environment
- The reputation of SEEDA and or organisations connected with it, - bringing them into disrepute or irreparably damaging working relationships between them.
- Breaches of confidentiality and security

7. Desktop/Laptop Security

7.1 At the end of the working day, all users should switch off their desktop computers and peripherals (including monitor) before leaving the premises, unless instructed not to by the IT department.

7.2 All mobile assets, such as PDAs/ Blackberries should not be kept locked in desks. They should be in the possession of the owner whenever possible and out of sight until needed.

7.3 All removable media from non-SEEDA sources must be scanned for virus by the IT department before it is used on any SEEDA system.

7.4 Users who infect any system with computer viruses though lack of care or malicious intent may be subject to disciplinary action.

7.5 Desktop PCs should have at least 15 cm of free space surrounding all parts of the system in order to maintain safe operating temperatures.

7.6 Flammable objects or any liquids should be kept well away from computers at all times.

7.7 Deliberately tampering with or modifying any SEEDA computer configuration without authorisation from the IT department may be regarded as committing a gross breach of rules.

7.8 Users must not open IT equipment, attempt repairs, fit replacement or enhancement parts or otherwise tamper with equipment.

7.9 Swapping of IT equipment is only permitted by IT staff (e.g. monitors, keyboards, mice)

7.10 All users should "lock" their sessions using the CTRL/ALT/DELETE combination, whenever they leave their computer unattended.

7.11 IT Portable devices such as Laptops, PDAs or Blackberries which are assigned to users must not be used by anyone other than the employee to whom it is issued.

7.12 By taking and using a portable device away from SEEDA premises the employee agrees to be responsible for ensuring it will be used only in circumstances appropriate to the requirements of health and safety.

Acknowledgement *I have received a copy of this SEEDA Acceptable Use for Desktop/Laptop computer systems, E-mail, Internet and Intranet policy and have read it and understood it.*	_____ Print Name _____ Signed _____ Date