Adamus Resources
Limited

INFORMATION SECURITY POLICIES AND STANDARDS FOR ALL USERS

1 use of E-mail

1.1 Access

1.1.1 All requests for use of e-mail services must be submitted to the head of the respective Department/Business Unit for approval.

1.1.2 Once approved, a call must be logged with the Helpdesk.

1.2 Business Use

1.2.1 The use of e-mail for Adamus business use must be within, but not limited to, the following constraints.

1.2.1.1 Employees may not use e-mail for personal commercial purposes.

1.2.1.2 Access to e-mail from a company-owned home-based computer or through company-owned connections must adhere to all the same standards that apply to use from within Adamus facilities.

1.2.1.3 Employees shall not allow family members or other non-employees to access Adamus e-mail systems via linked home computers.

1.2.1.4 Personal accounts with Internet Service providers should not be used from company computers.

1.2.2 The following is also prohibited.

1.2.2.1.1 Unauthorized attempts to break into any computer.

1.2.2.1.2 Theft or copying of electronic files without permission

1.2.2.1.3 Sending company files outside the company or inside the company to unauthorized personnel.

1.3 Personal Use

1.3.1 Adamus understands and recognizes that e-mail has become an acceptable and popular method for “communication” with parties associated directly with ADAMUS business and also with parties on a personal level. Adamus therefore allows **incidental** and **infrequent** personal use of e-mail on the following conditions.

1.3.1.1 It does not consume significant amounts of the user’s workday.

1.3.1.2 It does not consume substantial amounts of Adamus bandwidth in such a way that it negatively impacts upon Adamus e-mail system, either directly or indirectly. Adamus bandwidth could be impacted by distribution of the following.

1.3.1.2.1 Large e-mail messages. Users should consider using compression utilities such as Zip before sending large e-mail messages.

1.3.1.2.2 Attachment types such as JPEG, JPG, AVI, etc.

1.3.1.2.3 Chain letters, jokes, bitmaps, etc.

1.3.1.3 It does not expose Adamus to a noticeable increase in costs.

1.3.1.4 It does not expose Adamus to reputation or financial risks.

1.3.2 Adamus may, in its sole discretion and from time to time determine:

1.3.2.1 the content and mail size that is prohibited from being dispatched or received;

1.3.2.2 the maximum allowed disk space for individual mailboxes on the e-mail server.

1.4 **Privacy Expectation**

1.4.1 As Adamus allows the incidental and infrequent personal use of e-mail, users must be aware of the restrictions placed on the privacy of e-mail as follows.

1.4.1.1 Electronic mail is private and owned by the sender and each recipient account holder.

1.4.1.2 Adamus reserves the right to monitor e-mail received and sent by users to ensure proper content, and to detect security violations.

1.4.1.3 The contents of e-mail will not be monitored, censored, or otherwise examined except:

1.4.1.3.1 with specific authorisation from the head of the Department/Business Unit or as part of the required system administration;

1.4.1.3.2 when a Court order or law enforcement investigation requires the examination and release of any document, including electronic files such as e-mail;

1.4.1.3.3 when special conditions exit for users who receive e-mail associated with his/her job responsibilities and where the user's direct supervisor or others in the department have a business need to have access to their e-mail.

1.4.1.3.4 The IT Department will continue to maintain the privacy of mail, but, on authorization from the business unit manager, may locate and copy specific messages.

1.5 **Prohibited Use**

1.5.1 The creation, transmission, receipt or storage of certain content may be in violation of regulatory and statutory requirements and are therefore prohibited within Adamus. This content includes, but is not limited to the following.

1.5.1.1 Threats.

1.5.1.2 Pornographic or sexually explicit material.

1.5.1.3 Material containing derogatory racial, gender, religious or hate-oriented comments.

1.5.1.4 Defamatory remarks, including defamation of character and libellous remarks about products or other companies.

1.5.1.5 Discriminatory language or remarks that would constitute harassment of any type.

1.5.1.6 Any other comment that offensively addresses someone's age, sexual orientation, political beliefs, national origin, or disability.

1.6 **E-mail Etiquette**

1.6.1 Any form of communication is most effective if it conforms to etiquette acceptable to both the sender and the recipient of the message. Therefore, the following principles should be followed when using e-mail.

1.6.1.1 Be concise - long messages often lose their emphasis. If you have received a message as a part of a group of recipients, consider a reply to only the author rather than to the entire group.

1.6.1.2 As with any written form of communication, attention to proper grammar, spelling, etc. will convey your message most effectively.

1.6.1.3 Remember that even though the medium is electronic, the recipient of the message is another person.

1.7 **Representing Adamus - Vicarious Liability**

1.7.1 Users must be aware that in using Adamus e-mail facilities they are representing Adamus. It is therefore important that the use of e-mail is in accordance with the following.

1.7.1.1 Users should consciously build and preserve Adamus image when they use e-mail for communication.

Users should attach the official Adamus headers and disclaimers to e-mail

1.7.1.2 The creation of business e-mail is equivalent to the creation of any other company document. Therefore, users must use the same degree of care and seriousness associated with the drafting of company documents when composing business e-mail messages.

1.7.1.3 Users are not allowed to enter into any contractual agreement for or on behalf of Adamus using e-mail.

1.8 **Electronic Fraud**

1.8.1 As electronic fraud may be possible via e-mail, users must adhere to the following.

1.8.1.1 Impersonation of another user when using e-mail is prohibited within Adamus.

1.8.1.2 Users should not allow others to use their e-mail accounts. If a user has no option but to allow this, the user must understand that he/she will be held responsible for all actions performed on their e-mail account.

1.8.1.3 Anonymous e-mail may be used in the following circumstances.

1.8.1.3.1 A user reporting an incident due to wrongdoing caused by another Adamus user may send anonymous e-mail.

1.8.1.3.2 Users requesting medical information, without disclosing their identity.

1.9 **Intellectual Property**

1.9.1 Due to the legal restrictions placed on the copying and distribution of intellectual property, users must adhere to the following.

1.9.1.1 Users must not distribute material that has copyright, in such a way that the copyright is infringed.

1.9.1.2 Users must obtain prior permission from the author before copying or distributing content, this includes images and text found on web sites.

1.9.1.3 A user may quote interesting material, without prior permission, as long as the source is acknowledged.

1.10 **Computer Viruses**[1]

1.10.1 When receiving e-mail from an unknown source user must:

1.10.1.1 ensure that all e-mail attachments are scanned for viruses before opening, using approved Adamus anti-virus software;

1.10.1.2 immediately report any detection of a virus or malfunction that might be related to a computer virus to the Helpdesk;

1.10.1.3 when accessing public e-mail servers (e.g. Hotmail) or when connecting to public SMTP servers (e.g. Mweb) from a workstation that is linked to the Adamus network, ensure that any attachments are scanned for viruses on the user's workstation.

1.11 **Transmitting Confidential Information**

1.11.1 **Addressing E-mail**

1.11.1.1 When a user sends e-mail, it is the user's responsibility to ensure that the e-mail address of the recipient is correct.

1.11.1.2 When a user recognises that a mail item has been incorrectly addressed to him/her, the user should inform the sender by returning and deleting the mail.

[1] See also 4.6 **Software and Viruses** below

1.11.1.3 The user must ensure that his/her personal information on directories and/or address books is kept up to date.

1.11.2 Information Protection[2]

1.11.2.1 Prior to e-mailing or forwarding proprietary data the e-mail options should be set to confidential.

1.11.2.2 The message should be given the subject “Confidential”.

1.11.2.3 Documents containing proprietary information should be individually password protected.

1.11.2.4 The sender and receiver should agree on the password by calling in advance. Under no circumstances should sensitive information be sent without a password.

1.11.2.5 The sender should also ensure that the receiver is able to retrieve the message from the e-mail address to which it is sent – in terms of the software used to create the e-mail as well as any attached documents.

1.11.2.6 The e-mail system should not be used to communicate details of the password.

1.11.2.7 The message recipient should be asked to confirm receipt of the document.

1.11.2.8 Subject to the availability of encryption software, users must adhere to the following[3].

1.11.2.8.1 Users may send Adamus information to others who are on public e-mail systems. However, when transmitting private, confidential, critical or restricted Adamus information over public networks (for example, through the Internet) it must be encrypted (subject to the availability of software). This will help to provide confidentiality and integrity.

1.11.2.8.2 All encryption must be in accordance with the **Encryption Standard** (Schedule B).

1.11.2.8.3 Methods of encryption to be used will be determined by the IT Department and these may vary from time to time.

[2] See also Section 4 **PROTECTION OF INFORMATION** below

[3] See also 4.5 **Encryption** below

1.11.2.8.4 Users must be aware that certain infrastructures need to be in place to enable secure e-mail. Users can contact the Helpdesk for more information.

1.12 **E-mail Software**

1.12.1 Only e-mail software authorized by the IT department may be used - no re-mailer (mail bomber) software will be permitted for any purpose.

1.13 **Retention of E-mail Messages**

1.13.1 E-mail shall be retained for periods that would normally apply to written, typed or facsimiled transactions. Where precise retention periods need to be defined, they should be defined in conjunction with Adamus Legal Department.

1.14**Disclaimer of Liability**

1.14.1 Adamus is not responsible for material viewed or received by users from the Internet or other public e-mail systems. Users are cautioned that these communications may include offensive, sexually explicit, and/or other inappropriate material. Having an e-mail address may lead to receipt of unsolicited messages containing offensive content. Users are responsible for material viewed or received by them under their logon password.

2 use of internet / intranet

Adamus sees the Internet/Intranet as significant tools for business benefit and for achieving required business objectives. For example, the Internet can be used to access a wealth of information and resources, while the Intranet is one of the most effective ways of making Adamus information available internally to the organization. These services do however offer the opportunity for abuse of resources and inappropriate use of these mediums could expose Adamus to significant risks. Therefore, Internet/Intranet facilities will only be available to users after the acknowledgement of receipt at the beginning of the schedule has been signed. Any exceptions will be filed.

2.1 Access to the Internet

2.1.1 All requests for an Internet ID in order to access the Internet must be submitted to the head of the respective Department/Business Unit for approval.

2.1.2

2.1.3 Once approved, a call must be logged with the Helpdesk.

2.1.4

2.2 Business Use

2.2.1 Use of the Internet/Intranet for Adamus business use must be within, but not limited to, the following constraints.

2.2.1.1 Employees may not use the Internet for personal commercial purposes.

2.2.1.2 Access to the Internet/Intranet from a company-owned home-based computer or through company-owned connections must adhere to all the same standards that apply to use from within Adamus facilities.

2.2.1.3 Employees may not run tools/programs against any Internet system or server.

2.2.1.4 Employees shall not allow family members or other non-employees to access Adamus computer systems via linked home computers.

2.2.1.5 Personal accounts with Internet Service providers should not be used from company computers.

2.2.2 Unauthorized use includes, but is not limited to, the following.

2.2.2.1 Unauthorized attempts to break into any computer (hacking and cracking).

2.2.2.2 Theft or copying of electronic files without permission.

2.2.2.3 Sending or posting company files outside the company or inside the company to Unauthorized personnel.

2.3 Personal Use

2.3.1 Adamus understands and recognizes that the Internet has become an acceptable and popular method for researching and obtaining information and for communicating with certain service providers such as banks, etc. Adamus therefore allows **incidental** and **infrequent** personal use of the Internet/Intranet on the following conditions.

2.3.1.1 It does not consume significant amounts of the user's workday.

2.3.1.2 It does not consume substantial amounts of Adamus bandwidth in such a way that it negatively impacts upon Adamus systems, either directly or indirectly. Adamus bandwidth could be impacted by distribution of, for example:

2.3.1.2.1 Attachment types such as JPEG, JPG, AVI, etc.;

2.3.1.2.2 Chain letters, jokes, bitmaps, etc.

2.3.1.3 It does not expose Adamus to a noticeable increase in costs.

2.3.1.4 It does not expose Adamus to reputation or financial risks.

2.4 Additional Prohibited Use

2.4.1 The accessing and / or carrying of any obscene, defamatory or discriminatory material, including the following, is prohibited.

2.4.1.1 Pornographic or sexually explicit material.

2.4.1.2 Bestiality.

2.4.1.3 Material containing derogatory racial, gender, religious or hate-oriented comments.

2.4.1.4 Defamatory remarks, including defamation of character and libellous remarks about products or other companies.

2.4.1.5 Discriminatory language or remarks that would constitute harassment of any type.

2.4.2 Users of Adamus Internet system who discover they have connected with a web site that contains any of the material noted above must immediately disconnect from that site.

2.4.3 The ability to connect with a specific web site does not in itself imply that users of Adamus systems are permitted to visit that site.

2.5 Password Management

2.5.1 Internet/Intranet access to General Support systems and Public data shall require a password.

2.5.2 Password creation and usage must be in accordance those standards outlined in 4.4 below.

2.6 Downloading content

2.6.1 Users are permitted to download content from the Internet/Intranet. The downloading of content from the Internet/Intranet must however be in accordance with the following.

2.6.1.1 Users downloading large volumes should consider scheduling these for transmission after normal working hours.

2.6.1.2 When non-text files (databases, software object code, spreadsheets, formatted word-processing package files, etc.) are downloaded from non-Adamus sources via the Internet, the following conditions must be adhered to.

2.6.1.2.1 Files must be screened with approved virus detection software prior to being used (opened).

2.6.1.2.2 Downloading of software is only permitted under the direct control of the System Administrator.

2.6.1.2.3 Whenever an external provider of the software is not trusted, downloaded software should be tested on a stand-alone non-production machine that has been recently backed up. If this software contains a virus, worm, or Trojan horse, then the damage will be restricted to the machine involved.

2.6.1.2.4 Downloaded files must be decrypted and decompressed before being screened for viruses.

2.6.1.2.5 The use of digital signatures to verify that unauthorized parties have not altered a file is recommended, but this does not assure freedom from viruses.

2.7 Representing Adamus

2.7.1 Users must be aware that in using Adamus Internet/Intranet facilities they are representing Adamus. It is therefore important that the use of Internet/Intranet must be in accordance with the following.

2.7.1.1 Users should build and preserve Adamus image when using the Internet/Intranet.

2.7.1.1.1 Users may indicate their affiliation with Adamus in mailing lists (list servers), chat sessions, and other offerings on the Internet. This may be done by explicitly adding certain words, or it may be implied, for instance via an electronic mail address. In either case, whenever users provide an affiliation they must also clearly indicate the opinions expressed are their own, and not necessarily those of Adamus.

2.7.1.1.2 Users can indicate that opinions expressed are their own by the use of a disclaimer stating the following:

“The following are only my opinions, and do not reflect those of my employer”.

2.8 Posting Information on the Intranet

2.8.1 Designated owner

2.8.1.1 All information posted to the Adamus Intranet must have a designated "owner".

2.8.1.2 Contact information for this owner must be clearly indicated on the page where the information appears.

2.8.2 Approval for postings

2.8.2.1 Before any information is posted to the Adamus Intranet, approval must be obtained from the head of the Department/Business Unit in charge of the relevant

Intranet page and the owner of the information (or creator of the information if the owner has not yet been designated).

2.8.3 Posting Information

2.8.3.1 When posting information on the Intranet users must comply with the standards contained in the Schedule. Although the Intranet is an informal internal communications environment, the laws for copyrights, patents, trademarks, and the like still apply. To uphold these rights, and also to ensure the quality and security of the Intranet, users may post material to the Intranet only after complying with the following steps.

2.8.3.1.1 If material to be posted originates outside Adamus, written permission from the source must first be obtained, and the source must be given adequate credit.

2.8.3.1.2 If copyright infringement, confidential information disclosure, defamation of character, and/or other possible legal issues could be involved, Adamus legal counsel must first approve the posting.

2.8.3.1.3 Users must independently confirm the material's accuracy, timeliness, and relevance to Adamus business.

2.8.3.2 Users posting to Usenet newsgroups, Internet mail listings, etc. must include a company disclaimer as part of each message.

2.9 Information Protection[4]

2.9.1 Proprietary information must not be sent over the Internet unless it has first been encrypted by approved methods.

2.9.2 All encryption must be in accordance with Adamus **Encryption Standard** (Schedule B)[5].

2.9.3 User IDs and passwords, and other parameters that can be used to gain access to Adamus information must not be sent over the Internet in readable form.

2.9.4 In keeping with the confidentiality agreements signed by all users, Adamus software, documentation, and all other types of internal information must not be sold or otherwise

[4] See, too, Section 4 **PROTECTION OF INFORMATION** below.

[5] See, too, Section 4.3 below.

transferred to any non-Adamus party for any purposes other than business purposes expressly authorized by management.

2.9.5 Users should not allow others to use their user IDs and passwords when connecting to Internet sites requiring authentication (e.g. Gartner research database). If a user has no option but to allow this, the user must understand that he/she is the responsible party.

2.10Expectation of Privacy

2.10.1 On the Web, one of the real dangers is a possible loss of privacy or leakage of information about user activities. Employees should be aware of the following issues relating to their privacy when surfing the web.

2.10.1.1 When you visit a Web site, the site you are visiting can identify where your Internet connection originates. For example, if you use the Web from work, your activities can be identified as coming from Adamus.

2.10.1.2 Web sites can log all of your activity including any personal data you provide. The web site owner can associate you with this data on future visits. They may want to use this information to give you a better web experience, or they may be collecting competitive information, or both. Some web sites do not respect data privacy laws and may make the information collected from you available to other organizations.

2.10.1.3 Therefore, activities may be subject to monitoring, recording, and periodic audits to ensure they are functioning properly and to protect against Unauthorized use. Users must therefore note the following.

2.10.1.3.1 Adamus reserves the right to monitor sites (e.g. duration and content) visited by users and to detect security violations.

2.10.1.3.2 Adamus reserves the right to examine and access all information, created, stored or communicated using Adamus information systems whenever warranted by a business need or legal requirements.

2.10.1.3.3 Adamus will disclose information obtained through such examinations to appropriate third parties, including law enforcement agencies.

2.11Internet Integrity

2.11.1 When using the Internet all users must comply with the following.

2.11.1.1 All information taken off the Internet should be considered suspect until confirmed by separate information from another source.

2.11.1.2 Before users release any authorized internal Adamus information, enter into any authorized contracts, or, with permission, order any products via public networks, the identity of the individuals and organizations contacted must be confirmed.

2.12Electronic Fraud

2.12.1 Impersonating, misrepresenting, obscuring, suppressing, or replacing a user's identity on the Internet or any Adamus electronic communications system is forbidden.

2.13World Wide Web (WWW) - Browsing the Internet

2.13.1 Approved sources for licensed WWW software will be made available to users.

2.13.1.1 Only Adamus approved versions of browser software may be used.

2.13.1.2 Software for browsing the WWW is provided to employees for business use only.

2.13.1.3 All software used to access the WWW must be approved by the Information Technology (IT) Department and must incorporate all vendor-provided security patches.

2.13.1.4 Users are prohibited from changing the configuration of their web browsers, including the following.

2.13.1.4.1 Changing the firewall http proxy.

2.13.1.4.2 Enabling active content such as ActiveX, Java and Java Script.

2.14**General**

2.14.1 Users are not allowed to create personal web pages using the company’s facilities (systems, network or computers).

2.14.2 User are not permitted to operate an independent web page.

2.14.3 Running an online business for personal gain using the company’s facilities is forbidden during and outside of business hours.

2.14.4 Users must not copy software from the Internet. This includes the use of freeware and shareware (certain terms and conditions normally apply). Any users requiring such software to perform their job must contact the IT Department for permission and assistance.

2.15Disclaimer of Liability

2.15.1 Adamus is not responsible for material viewed or downloaded by users from the Internet or other public communications networks. Users are cautioned that web pages may include offensive, sexually explicit, and/or other inappropriate material. Users accessing the Internet and other public communications networks do so at their own risk.

3 Use of Networking Facilities

3.1 **Use of** VPN access

3.1.1 All request for remote access (VPN) to Adamus network must be done in writing and must be approved by the relevant business owner and the IT manager / coordinator.

3.1.2 Persons using remote access to an Adamus information resource must be individually identified and authenticated by an independent dedicated device such as a network access controller.

3.2 VPN Access Control

The Benefits
Reduce downtime due to unauthorized changes
Application security- changes will be logged for any change/update on system
Control on access to system
All changes to be documented

The Risks

Risks of not implementing the solution:

Not implementing this control will result in vendors accessing the Application and no control on any changes/updates are documented.

Controls

All accounts to remain disabled
If a 3'd party support person has to perform tasks for Adamus a call must be logged by the
Business owner requesting access and then a change/incident to be logged for the tasks to be performed.
If a call and change has been logged, the account must be enabled and disabled at the exact times.
If a 3'd party support person needs more time the Business owner must extend the change / incident to extend the access window

If a 3'd party finds that additional changes NEED to be made in order to perform the tasks, these

changes should be sent through to the Business Owner for approval. These extra changes will be documented.

All documentation to be kept for Audit purposes

3.3 Establishing Networks

3.3.1 Users must not establish electronic bulletin boards, local area networks, modem connections to existing internal networks, or other multi-user systems for communicating information without the specific approval of the IT Department and the owner of these systems.

3.4 Unauthorized Browsing

3.4.1 Users must not browse through Adamus computer systems or networks. For example, curious searching for interesting files and/or programs in the directories of other users is prohibited.

3.4.2 Steps taken to legitimately locate information needed to perform one's job are not considered as Unauthorized browsing.

3.5 **General**

3.5.1 When connected to and using Adamus internal networks, including Local Area Networks (LANs):

3.5.1.1 do not misrepresent yourself (i.e., masquerade) as someone else on the network;

3.5.1.2 do not monitor network traffic (i.e., use a "sniffer" or similar device) without first obtaining explicit management approval and informing your IT Department;

3.5.1.3 do not add any network device, which creates an external connection (e.g. a bridge, router, gateway, hub, modem) to your workstation without first obtaining permission from the IT department.

3.5.1.4 do not install file sharing or peer-to-peer software (e.g. "Torrent") unless Adamus provides it. Sharing files on your own hard drive (via network connections) can pose the following threats.

3.5.1.4.1 Unauthorized access to data files.

3.5.1.4.2 Damage to data/program files - either accidental or malicious.

3.5.1.4.3 Damage caused by virus attacks.

3.5.1.4.4 If you must allow other users to access or store files on your network connected workstation you must select either User ID access control or password access control when defining the share options for the workstation disk drives and files.

3.6 You must not allow ANONYMOUS FTP, TFTP, or other unauthenticated access to program or data files on your workstation.

4 Protection of information, hardware and software

4.1 Clean Desk

4.1.1 **General Controls** pertaining to a clean desk include the following.

4.1.1.1 Where appropriate, paper and computer media must be stored in suitable locked cabinets and/or other forms of security furniture when not in use, especially outside working hours.

4.1.1.2 Incoming and outgoing mail points and unattended fax machines should be protected.

4.1.1.3 Proprietary business information should be locked away when not required, especially when the office is vacated.

4.1.1.4 Proprietary information, which has been printed, should be cleared from printers immediately.

4.1.2 **Desktop confidentiality -** To promote desktop confidentiality the following must be adhered to:

4.1.2.1 In an open plan office user must be aware of Unauthorized users reading information displayed on their screen.

4.1.2.2 Users must switch off their computer when it will be left unattended for an extended period of time. Boot up and or hard drive protect passwords must be used.

4.1.2.3 No obvious links or shortcuts to sensitive documentation must be created, e.g. shortcut for “Marketing Information.doc” on the Windows desktop.

4.1.2.4 All Windows desktop backgrounds must be in accordance with Adamus standards.

4.1.2.5 No proprietary information must be posted on the computer screen, i.e. with post-it stickers.

4.2 Clear Screen

4.2.1 **Screensavers**

4.2.1.1 A password protected screen saver will obscure the content of your computer screen after a period of no activity. Use of screensavers must be used in accordance with the following.

4.2.1.1.1 Users must enable screensavers on their computers, which will require input of a password if inactive for more than 5 minutes.

4.2.1.1.2 Users must use screensavers which do not offend, intimidate or disparage others.

4.2.1.1.3 Users must change their screensaver password regularly, e.g. every 30 days.

4.2.1.1.4 Users are not allowed to disclose their screensaver password to any personnel without authorization from their direct supervisor at Adamus.

4.2.1.1.5 When entering passwords users must prevent Unauthorized observation by any third party, e.g. shoulder surfing.

4.3 Computer lockout

4.3.1 Users must lock out of their workstation(s) and any active applications when leaving their computers unattended.

4.3.2 Users must not disclose their passwords to any Unauthorized personnel.

4.3.3 Users must ensure they have logged out of all systems, including the network, after hours.

4.4 Passwords

4.4.1 Temporary passwords assigned to users must be changed at first log-on.

4.4.2 Creating Passwords

4.4.2.1 Passwords must be a minimum of eight (8) characters in length and must comprise letters, numbers, and special characters.

4.4.2.2 Each password must contain at least one capital letter and one numeric.

4.4.2.3 An ideal password is created from a pass phrase. For example: The phrase "Ghana to win the World Cup" might result in the password of "gh2wtwc!" by using the first letter of each word in the phrase, the number 2 for "to" and adding the exclamation mark.

4.4.2.4 Passwords must not be easily associated with Adamus or the user (identification number, employee number, address, numerical equivalent of name, family names, birthdate, spouse name, pet names etc.).

4.4.2.5 Passwords must not contain:

4.4.2.5.1 words from a dictionary, movie or geographical location; and
4.4.2.5.2 common character sequences such as “123456”.

4.4.2.6 Passwords should not be based upon month/year combinations such as "jan01" or "april2001". ‘Hackers’ use these types of words in attempts to guess passwords.

4.4.2.7 Users will not use cyclical passwords. For example, users cannot add a numeric at the end of the password in sequence.

4.4.2.8 Passwords must not consist of identical all numeric or all alphabetic characters, for example 1111111 or aaaaaaa.

4.4.3 Safeguarding Passwords

4.4.3.1 A password must be known only to the user who creates it.

4.4.3.2 Passwords must not be shared with others except in a temporary emergency situation.

4.4.3.3 If a situation requires a password to be revealed to a second person, the owner of the password must change the password as soon as possible after the emergency situation has passed.

4.4.3.4 Passwords must not be stored in readable form (i.e. writing down passwords).

4.4.3.5 Passwords should be changed every 30 days or, whenever there is any indication that the user’s password has been compromised, passwords must be changed promptly but no later than within one working day.

4.4.4 **Identification Requirements**

4.4.4.1 User IDs may not be utilized by anyone but the individual to whom the ID has been assigned.

4.4.4.2 Access to a system may be disabled or suspended if a user has not used their system capability within a sixty-day period.

4.4.4.3 A user must not program a password into a device in order to avoid manually entering that password at time of logon.

4.5 Encryption

4.5.1 All computerized confidential and/or critical information must be encrypted consistent with Adamus **Encryption Standard** when not in active use (for example, when not manipulated by software or viewed by an authorized user). Users must contact the Helpdesk should they require help in this regard.

4.5.2 Traffic (data or information) travelling over computer or voice (telephone) networks is subject to interception and/or eavesdropping. Therefore, users must encrypt proprietary information when transmitting over the network.

4.6 Malicious Software and Viruses

4.6.1 Virus detection programs will be loaded onto all computers.

4.6.2 Users must however check that the latest version of the virus detection program is installed on their computers when they receive it from the Information Technology (IT) Department.

4.6.3 Users are not allowed to remove or de-activate virus detection programs installed on their computers, without approval from the IT Department.

4.6.4 **Preventing Viruses**

4.6.4.1 Externally supplied, CD-ROMs, and other removable storage media must not be used unless they have first been checked for viruses.

4.6.4.2 Externally supplied computer-readable files (software programs, databases, word processing documents, spreadsheets, etc.) must be unzipped prior to being subjected to an approved virus checking process.

4.6.4.3 If the files have been encrypted, they must be decrypted before running a virus detection program. Many virus detection programs cannot detect viruses in a zipped or encrypted file.

4.6.5 Eradicating Viruses

4.6.5.1 Because viruses can be complex and sophisticated, users must not attempt to eradicate them without expert assistance.

4.6.5.2 If users suspect infection by a virus, they must immediately stop using the involved computer, disconnect from all networks, and call the Helpdesk.

4.6.5.3 If the suspected virus appears to be damaging information or software, users must turn the computer off immediately.

4.6.6 Playing with viruses

4.6.6.1 Users must not intentionally write, compile, copy, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any Adamus computer system. Such software may be called a virus, bacteria, worm, Trojan horse, etc.

4.6.7 General

4.6.7.1 Users must not open e-mail attachments from unknown sources. All e-mail attachments received from known sources must be scanned for viruses.

4.6.7.2 Executable attachments (i.e. .exe) must not be launched and should be deleted immediately.

4.6.7.3 All software and/or freeware downloaded from the Internet or attachments from mail programs used on the Internet must be scanned for viruses.

4.6.7.4 All users must ensure that they have Anti-virus software enabled on their computers, and that virus software upgrades (as distributed electronically) are applied. The IT Department should be contacted if the user is unsure.

4.6.7.5 It is the user’s responsibility to check all external material for viruses – this includes e-mails with attachments, and disks from external sources.

4.6.7.6 It is prohibited for employees to create and distribute dangerous code of any form within or to the company and its associates.

4.7 Back-up of Information

4.7.1 All proprietary and/or valuable information resident on Adamus computer systems must be periodically backed-up. Such back-up processes must be performed at least weekly.

4.7.2 Unless automatic back-up systems are known to be operational, all end-users are responsible for making back-up copies of sensitive, critical, or valuable files. These separate back-up copies should be made each time that a significant number of changes are saved.

4.7.3 Users must ensure the back-up process was successful by restoring selected files from back-ups made.

4.7.4 Access to back-up copies should be properly restricted; e.g. storage media such as disks, etc. should be locked-up and access to back-up drives should be set up with user profile access control links.

4.8 Labelling, saving and destruction of information

4.8.1 **Labelling of information –** All information must be labelled in accordance with the following guidelines.

4.8.1.1 Proprietary information should be labelled (marked) with an appropriate classification from the time when it is created until it is destroyed or declassified.

4.8.1.2 The hardcopy version of the information as well as the labels on the storage media containing the information (floppy disks, CD-ROMs, etc.) must be marked.

4.8.1.3 Proprietary information should also be marked with an instruction on how the printout is to be stored, transported and disposed of should it be printed.

4.8.2 Saving Information

4.8.2.1 Make back-up copies of essential business information and software regularly.

4.8.2.2 Regularly test back up media.

4.8.2.3 Store back up media in a location that is unlikely to be affected by the same disaster.

4.8.3 Destruction of information

4.8.3.1 **Deletion of Information**

4.8.3.1.1 Users are required to delete information from their computers if it is clearly no longer needed or potentially useful.

4.8.3.1.2 Prior to deleting any Adamus information, users should consult the Documented Retention Schedule prepared by Adamus Legal Department (for archiving of information).

4.8.3.1.3 Use of an "erase" feature (e.g. putting a document in a trash can icon) is not sufficient for proprietary information because the information may still be recoverable.

4.8.3.1.4 Proprietary information should be deleted via an overwrite (zeroization) program approved by the IT Department.

4.8.3.1.5 All disks and CDs must be formatted before given to any third party or employee of Adamus not authorized to see content. Users should contact the Helpdesk for assistance on formatting disk and CDs after authorization has been obtained from the owner of the information.

4.8.3.2 Destruction of Information

4.8.3.2.1 *Electronic Media*

4.8.3.2.1.1 Prior to disposal, defective or damaged disks containing proprietary information must be destroyed using scissors or other methods approved by the IT Department.

4.8.3.2.2 *Hardcopy Information*

4.8.3.2.2.1 All hardcopies containing proprietary information must be disposed of via a shredder or other methods approved by the IT Department.

4.9 Effecting Changes

4.9.1 Changes to Software

4.9.1.1 Only software packages which appear on the Adamus list of permissible software packages can be run on user's computers.

4.9.1.2 Users may not install other software packages on their computers without obtaining advance permission from the IT Department.

4.9.1.3 Users must not permit automatic software installation routines to be run on Adamus computers unless the IT Department has first approved these routines.

4.9.1.4 Auto discovery license management software may be used to remotely determine which software packages are resident on users' hard disks. Unapproved software may be removed without giving user advance notice.

4.9.1.5 Users are not allowed to download and install software, games and/or freeware from the Internet.

4.9.2 Changes to Operating System Configurations

4.9.2.1 Users must not change their computer operating system configurations by, for example, upgrading existing operating systems and / or installing new operating systems.

4.9.2.2 If such changes are required **and authorized**, they will be performed by Helpdesk personnel (in person or with remote system maintenance software).

4.9.3 **Changes to Hardware**

4.9.3.1 Computer equipment supplied by Adamus must not be altered or added to in any way (for example, with upgraded processor, expanded memory, or extra circuit boards) without the prior knowledge of and authorization from the IT Department.

4.10 Asset Accountability

4.10.1 **Generally**

4.10.1.1 Users must not leave proprietary information unattended e.g. at a printer or on photocopy machines. All mail points, both incoming and outgoing, photocopiers and fax machines must be protected from unauthorized access.

Care must be taken during off hours to protect against improper usage of these resources.

4.10.1.2 All users must protect information in any format (hard copy, disk, tape, etc) at the level commensurate with its classification.

4.10.1.3 Users who handle proprietary or valuable information must position their computer screens in such a way that the information cannot be readily viewed through a window, by persons walking in a hallway, or by persons waiting in reception and related areas.

4.10.2 Software Assets

4.10.2.1 Users must protect personal computing device software from theft, Unauthorized use, and/or Unauthorized copying.

4.10.2.2 Users are not allowed to install or remove any software from any of Adamus computing equipment.

4.10.3 Hardware Assets

4.10.3.1 *Computing Equipment*

4.10.3.1.1 Users accountability for computing equipment must be in accordance with the following.

4.10.3.1.1.1 Users of laptops must ensure that they are protected by installing cable protection.

4.10.3.1.1.2 Users must not leave laptops unattended in an unsecured environment (on site or off-site).

4.10.3.1.1.3 Users must not leave laptops exposed in cars or hotel rooms.

4.10.3.1.1.4 User must never check-in a laptop as luggage when travelling. Always carry it on as hand luggage, in a briefcase or a laptop carry case. Airport X-ray machines do not damage data on a laptop or diskette.

4.10.3.1.1.5 Users must lock laptops in the car trunk when travelling.

4.10.3.1.1.6 Users must return any items issued to them (laptop computers, keys, ID cards, software, data, documentation, manuals etc.) to their manager or the Human Resources (HR) Department upon resignation or termination.

4.10.3.1.1.7 Equipment or software may not be taken off Adamus' premises without authorization. Authorization must be obtained from the IT Department.

4.10.3.1.1.8 Equipment and media taken off the premises should not be left unattended in public places.

4.10.3.1.1.9 Equipment must not be exposed to extreme heat or cold.

4.10.3.1.1.10 Avoid storing any devices (i.e. hard disks, etc) and equipment (i.e. laptops, desktops, etc) in automobiles. Automobiles and hotel rooms are potential theft areas.

4.10.3.1.1.11 Store devices out of the view of others.

4.10.3.2 *Computer Media*

4.10.3.2.1 Users must make use of reliable transport or couriers as specified by Adamus when transporting media.

4.11 **Voice Communication**

4.11.1 When using the telephone, especially a speakerphone, cell phone or public phone, to discuss sensitive information, users must ensure that their conversations cannot be overheard.

4.11.2 The leader of a telephonic conference call must ensure that only authorized individuals are connected to the call.

4.11.3 Use a cordless or cellular phone to discuss proprietary information can be an exposure. Use with discretion.

4.11.4 Security of Voice Mailboxes

4.11.4.1 Voice messaging systems and individual subscriber mailboxes are an attractive target for phone hackers. Voice messaging systems and/or individual mailboxes on such systems that have not been properly secured can result in Unauthorized retrieval of messages containing proprietary information, or mailboxes being commandeered for Unauthorized purposes. Users must:

4.11.4.2 Change their mailbox password as soon as they are notified the mailbox has been activated or reactivated.

4.11.4.3 Change their password at least every sixty days.

4.11.4.4 Use a password that is at least six characters long and does not contain sequential numbers or repeat the same numbers, e.g., 123 or 777.

4.11.4.5 Not share your password with anyone.

4.11.4.6 Not keep messages on the system longer than necessary, especially messages containing sensitive, confidential or personal information.

5 *intellectual property rights protection*

5.1 General

5.1.1 All personal computing device software must be obtained from approved sources, as defined by Adamus.

5.1.2 Software not supplied by Adamus or at Adamus direction must not be loaded or used on Adamus personal computing devices.

5.1.3 Obtaining or downloading of public domain and/or evaluation copies of software from other than Adamus sources is permitted only under the following conditions.

5.1.3.1 The software must be required for a legitimate business purpose and approved by management.

5.1.3.2 Use of the software must comply with all applicable copyright and license agreements.

5.1.3.3 At a minimum the person obtaining the software must perform an evaluation, as to the safety and reliability of the vendor or provider of the software.

5.1.3.4 The software should be checked for viruses and other malicious code. This evaluation should be done on a single system before deploying the software to others.

5.2 **Copyright Protection**

5.2.1 Adamus strongly supports strict adherence to software vendors’ license agreements and copyright holders’ notices.

5.2.2 Users must therefore strictly adhere to the following conditions.

5.2.2.1 Making Unauthorized copies of licensed and copyrighted software, even if only for “evaluation” purposes, is strictly forbidden.

5.2.2.2 Adamus allows reproduction of copyrighted materials only to the extent legally considered “fair use” or with the permission of the author/owner.

5.2.2.3 If users have any questions about the relevance of copyright laws, they should contact Adamus Legal Department.

5.2.2.4 Unless they receive information to the contrary, users should assume that software and other materials are copyrighted.

5.2.2.5 It is the responsibility of each employee to protect Adamus interests as they perform their duties. This includes responsibility for assuring that commercial software, acquired by Adamus, is used only in accordance with licensing agreements.

5.3 Rights to documents generated and programs developed by users

5.3.1 Without a specific written exception, all programs and documentation generated by, or provided by users for the benefit of Adamus are the property of Adamus.

5.3.2 Software developed by Adamus employees on company time becomes the property of Adamus.

6 Use of Resources

6.1 Physical Access to Adamus Premises

6.1.1 No person is allowed access to Adamus building without proper authorization.

6.1.2 Users must allow examination of access cards if requested by security personnel. Failure to comply may result in denial of access to the facility and/or removal from the facility.

6.1.3 Users authorized to enter a controlled access area must not allow unidentified, Unauthorized or unknown persons to follow them through a controlled access entrance.

6.1.4 Employees of Adamus with lost access cards will be required to sign in before access will be granted to Adamus facilities.

6.1.5 All personnel must keep their access cards secure and visible at all times.

6.1.6 Users with access to keys for secure facilities are accountable for the safe keeping of those keys as well as the information and facilities stored in the secure area.

6.1.7 Users must ensure that all windows are securely locked after hours as this will help prevent theft of equipment.

6.2 Equipment Theft

6.2.1 To prevent theft, where feasible and possible, all office desktop computers and mobile computers must be physically secured to desks with approved devices such as locking wires or plates that bolt the equipment to furniture. To obtain such devices the Helpdesk can be contacted.

6.2.2 All computer equipment is marked with a visible (asset tag) and invisible identification information on key components that clearly indicates it is Adamus property. Periodic physical inventories will be used to track the movement of computers and related computer equipment.

6.2.3 Offices should be locked when leaving computers and other computer equipment behind.

6.3 Custodians for Equipment

6.3.1 The primary user of a computer is considered a custodian for the equipment. If the equipment has been damaged, lost, stolen, borrowed, or is otherwise unavailable for normal business activities, the custodian must promptly inform the relevant Information Security Co-Ordinator's of the incident.

6.4 Moving Equipment

6.4.1 Computer equipment must not be moved or relocated without the knowledge and written approval of the IT department.

6.5 Use of Personal Equipment

6.5.1 Users must not bring their own computers, computer equipment, or computer software into Adamus facilities without prior authorization from their direct supervisor/manager.

6.6 **Property Pass**

6.6.1 Computers, portable computers and related information systems equipment must not leave Adamus offices unless accompanied by a property pass signed by a Department/Business Unit Manager. The property pass should contain the serial number of the equipment to be removed. Reference must be made to the appropriate waybill policy/practice in use at the location.

.

6.6.2 Equipment owned by users and brought into Adamus offices must also have a property pass containing serial numbers where possible. Users neglecting this requirement will discover that they are not able to remove their own equipment upon leaving the offices.

7 *Reporting and Responding to Security Incidents*

For more information, see standards

7.1 Identification of Security Incidents

7.1.1 Methods by which suspicious activity can be identified by a user include, but is not limited to:

7.1.1.1 unexpected account lockout;

7.1.1.2 unusual last login time;

7.1.1.3 unknown files in their file areas.

7.2 Reporting Security Incidents

7.2.1 All Adamus users must watch for any potential security incidents including:

7.2.1.1 breaches of confidentiality;

7.2.1.2 denial of service;

7.2.1.3 errors resulting from incomplete or inaccurate business data;

7.2.1.4 information system failures and loss of service.

7.2.2 Any such incidents must be promptly reported to the Helpdesk and/or the Local IS Co-Ordinator. This can be done in the way of a phone call or e-mail.

7.3 Reporting of Weaknesses

7.3.1 Users are required to note and report any suspected security weaknesses in, or threats to, systems or services.

7.3.2 Users must not attempt to prove a suspected weakness as testing weaknesses might be interpreted as a potential misuse of the system.

7.4 Reporting of Software Malfunctions

7.4.1 Prior to reporting software malfunctions the following actions should be considered by the user.

- The symptoms of the problem.

- Any messages appearing on the screen should be noted.
- Use of the computer should be suspended and the computer isolated.
- The computer should be disconnected from Adamus network.
- Disks, which were used on the affected computer, should not be transferred to any other computer.

7.4.2 Users must not attempt to remove the suspected software, unless authorized by the Adamus IT Department.

8 Protection against Social Engineering

8.1 Social engineering is the practice of impersonating someone else to gain information or services in a fraudulent manner. Employees must take steps to avoid being the victims of social engineering. Required steps include the following.

8.1.1 Know with whom you are communicating. If you do not know the caller personally or suspect the caller may not be valid, insist on a call-back number and before returning the call, verify that the caller is legitimate.

8.1.2 You can be “spoofed” via E-mail. The name and address you receive or send to via E-mail may not be the real name and address of the person. Do not send Adamus or customer proprietary information or reply with Adamus or customer proprietary information to E-mail addresses you do not know or cannot verify as correct.

8.1.3 Make sure that the caller has a business need to know the information they are requesting. Never furnish proprietary information until the caller's need to know has been established.

8.1.4 Users who become the victim of social engineering, or social engineering attempts must report the incident to the appropriate Adamus IT Department.

9 Access Rights of former-Users

9.1 Users whose connection with Adamus has been terminated have no right of access to any Adamus information systems and/or services.

SIGNED at …………………this ………day of ………………

………………………………..

Employee

……………………………….

Operation