Australian Graduate School of Leadership
Policy Register

Policy name	Information Technology		
Version	1.0	Status	Approved by Board of Directors
Communication	To all staff	Date	21 January 2013

Printing this document may render it out of date. Please refer to the latest online version at http://imia.edu.au/reference

Related Documents	• Policy – Internal Audit • Terms of Reference – Audit Committee

1. Preamble

The aim of this policy is to ensure that AGSL's information technology resources are adequate, appropriate and reliable for effective and efficient delivery of AGSL's services and other operational imperatives.

2. Scope

This policy applies to all computers and other equipment that are connected to the AGSL network via a standard network connection, wireless connection, modem connection, or virtual private network connection. This includes both company-owned computers and personally-owned computers attached to the AGSL's network. The definition of computers includes desktop workstations, laptop computers, handheld computing devices, and servers.

3. Principles

Anti-Virus

Currently, AGSL uses Microsoft Security Essential combined with Windows Firewall on all computers running Microsoft Windows 7 and earlier versions (Windows 8 and later versions come with integrated security and do not need additional software). Licensed copies of Microsoft Security Essentials can be obtained at http://windows.microsoft.com/en-US/windows/security-essentials-download. The

most current available version of the anti-virus software package will be taken as the default standard.

All computers attached to the AGSL's network must have standard, supported anti-virus software installed. This software must be active, be scheduled to perform virus checks at regular intervals, and have its virus definition files kept up to date.

Any activities with the intention to create and/or distribute malicious programs onto the AGSL network (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.) are strictly prohibited.

If an employee receives what he/she believes to be a virus, or suspects that a computer is infected with a virus, it must be reported to the COO immediately at coo@imia.edu.au. Report the following information (if known): virus name, extent of infection, source of virus, and potential recipients of infected material.

No employee should attempt to destroy or remove a virus, or any evidence of that virus, without direction from COO.

Any virus-infected computer, or any computer found not to have adequate virus protection installed, will be removed from the network until the situation has been rectified and permission from the COO granted to reconnect to the network.

Passwords

Passwords are an important component of information and network security. The use of a user id and password combination serves to identify and authenticate a user to system resources and information assets. It is only through authenticated access that the enterprise can be assured that systems and data are being used appropriately. As such, passwords must be constructed, used and protected appropriately to ensure that the level of security they imply is actually met.

The purpose of this policy is to provide the guidelines necessary for all of the employees of AGSL to create appropriate passwords and to use them and protect them in an appropriate manner.

Remote Access

The purpose of this policy is to define standards, procedures, and restrictions for connecting to AGSL's internal network(s) from external hosts via remote access technology, and/or for utilizing the Internet for business purposes via third-party wireless Internet service providers (a.k.a. "hotspots"). AGSL's resources (i.e.

corporate data, computer systems, networks, databases, etc.) must be protected from unauthorized use and/or malicious attack that could result in loss of information, damage to critical applications, loss of revenue, and damage to our public image. Therefore, all remote access and mobile privileges for AGSL employees to enterprise resources – and for wireless Internet access via hotspots – must employ only company-approved methods.

All remote access will be centrally managed by AGSL's COO and will utilise encryption and strong authentication measures. Remote access connections covered by this policy include (but are not limited to) Internet dial-up modems, frame relay, ISDN, DSL, VPN, SSH, cable modems, proprietary remote access/control software, etc.

All employees requiring the use of remote access for business purposes must go through an application process that clearly outlines why the access is required and what level of service the employee needs should his/her application be accepted. Application forms must be approved and signed by the employee's unit manager, supervisor, or department head before submission to the IT department.

Employees may use privately owned connections (under 'Supported Technology') for business purposes. If this is the case, the IT department must approve the connection as being secure and protected. However, the company's IT department cannot and will not technically support a third-party ISP connection or hotspot wireless ISP connection. All expense forms for reimbursement of cost (if any) incurred due to remote access for business purposes (i.e. Internet connectivity charges) must be submitted to the appropriate unit or department head. Financial reimbursement for remote access is not the responsibility of the IT department.

Personnel Security

By following defined protocols regarding staffing, AGSL ensures that the users to whom it extends information system access will understand and treat that access with appropriate regard for information security. The potential exists that, without these protocols, information system users will have insufficient regard for the security of the information systems or information they use, increasing the risk that AGSL is required to accept.

Security Infrastructure

Dedicated security infrastructure allows information systems to be provided a greater level of security than can be achieved through configuration control alone by delivering enhanced security capabilities. Without dedicated infrastructure the potential exists that security vulnerabilities that cannot be mitigated by the

capabilities inherent in AGSL's information systems will be exploited leading to compromise of information system security.

System Monitoring and Auditing

System monitoring and auditing is used to determine if inappropriate actions, either intentional or unintentional, have occurred within an information system. System monitoring is used to look for these inappropriate actions in real time while system auditing looks for them after the fact. Without system monitoring and auditing it can be difficult, if not impossible, to determine when a failure of the information system security, or a breach of the information systems itself has occurred, the magnitude of the breach or failure, and the details of that breach or failure.

Data Security

The goal of this section is to inform employees at AGSL of the rules and procedures relating to data security compliance. The data covered by this section includes, but is not limited to all electronic information found in e-mail, databases, applications and other media; paper information, such as hard copies of electronic data, employee files, internal memos, and so on.

IT Support

AGSL provides computer and information systems support for all staff members. The purpose of this section is to describe the basic level of service. It is also the purpose of this section to identify and delineate the limits of AGSL's IT support capabilities and what will not be supported.

"IT support" is defined as any queries made by end users regarding any failures, problems, issues, questions, and other matters relating to the operation and continuity of company-owned PCs, servers, Web sites, software, peripherals, telephony, mobile devices, and other equipments or assets.

The range of support offered will vary depending on the nature of the problem, the number of staff or resources available to resolve the problem, the criticality of the asset in question, and other factors regarding the nature of the support requested. Priority will generally be given to mission-critical applications/workflows/assets first, moving down in priority sequence.

IT Development

The role of IT is to support and facilitate business objectives. IT development initiatives must be in line with the general business strategy and direction.

Outsourcing

In some cases, it may be more cost efficient, convenient or expedient, or even in fact necessary, to outsource the development of IT initiatives. Where this is the case, the related IT projects may be required to be subject to a competitive tender process (see Accounting policy) and appropriate performance criteria and reporting procedures are to be established with the third-party organisation.

4. Procedures

Rules for Virus Prevention

Always run the standard anti-virus software provided by AGSL.

Never open any files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source.

Never open any files or macros attached to an e-mail from a known source (even a co-worker) if you were not expecting a specific attachment from that source.

Be suspicious of e-mail messages containing links to unknown Web sites. It is possible that the link is a malicious executable (.exe) file disguised as a link. Do not click on a link sent to you if you were not expecting a specific link.

Some file extensions are blocked by the e-mail system. If you have a business need to send a file of a type that is blocked by the mail server, contact the COO.

Never copy, download, or install files from unknown, suspicious, or untrustworthy sources or removable media.

Avoid direct portable drive (e.g. memory stick) sharing with read/write access. Always scan a portable drive for viruses before using it.

If instructed to delete e-mail messages believed to contain a virus, be sure to also delete the message from your Deleted Items or Trash folder.

Back up critical data and systems configurations on a regular basis and store backups in a safe place.

Regularly update virus protection on personally-owned home computers that are used for business purposes. This includes installing recommended security patches for the operating system and other applications that are in use.

Passwords

Password construction, lifecycle and re-use parameters will be variable according to the classification of the system or data that they are intended to protect.

Passwords should not be based on well-known or easily accessible information, including personal information, nor should they be words commonly found within a standard dictionary.

Users will be notified one week in advance of password expiration. At that point, and at every subsequent login until a change is made, users will be prompted to select a new password.

AGSL will use technical measures to ensure that users conform to the policy.

All passwords must conform to the guidelines outlined below.

Password Construction Guidelines

Passwords used to access data classified as “Secret” or the systems that host this data must be a minimum of ten (10) characters in length. Further, these passwords must use at least one character of the four character types, those being lower case letters, upper case letters, numbers and special characters.

Passwords used to access data classified as “Confidential” or the systems that host this data must be a minimum of eight (8) characters is length. Further, these passwords must use at least one character of three of the four character types, those being lower case letters, upper case letters, numbers and special characters.

Passwords used to access data classified as “Private” or the systems that host this data must be a minimum of six (6) characters in length. Further, these passwords must use at least one character of two of the four character types, those being lower case letters, upper case letters, numbers and special characters.

Passwords are not needed to access data classified as “Public” or the systems that host this data, as long as these systems do not host data of a higher classification level and so no construction guidelines need to be set.

Password Lifecycle Guidelines

Passwords used to access data classified as “Secret” or the systems that host this data will have a maximum age of one (1) month and a minimum age of one (1) month. As such, passwords must be changed every month and cannot be changed more frequently. Where the application or system can only be specified to change on the basis of a variable number of days, maximum and minimum age will be set at thirty (30) days.

Passwords used to access data classified as “Confidential” or the systems that host this data will have a maximum age of three (3) months and a minimum age of two (2) weeks. As such, passwords must be changed every three (3) months and cannot be changed more frequently than every two (2) weeks. Where the application or system can only be specified to change on the basis of a variable number of days, maximum age will be set at ninety (90) days and minimum age at fourteen (14) days.

Passwords used to access data classified as “Private” or the systems that host this data will have a maximum age of six (6) months and a minimum age of one (1) week. As such, passwords must be changed every six (6) months and cannot be changed more frequently than every one (1) week. Where the application or system can only be specified to change on the basis of a variable number of days, maximum age will be set at one hundred and eighty (180) days and minimum age at seven (7) days.

Passwords are not needed to access data classified as “Public” or the systems that host this data, as long as these systems do not host data of a higher classification level and so no lifecycle guidelines need to be set.

Password Reuse Guidelines

Passwords used to access data classified as “Secret” or the systems that host this data may never be reused once they have expired. As such a completely new password is required at each expiry. “Completely new” is defined as having at least fifty percent (50%) of the characters different from the previous password.

Passwords used to access data classified as “Confidential” or the systems that host this data may be reused every sixth password. As such a completely new password is required for the first five expiries; thereafter the first password can be reused. “Completely new” is defined as having at least fifty percent (50%) of the characters different from the previous password.

Passwords used to access data classified as “Private” or the systems that host this data may be reused every third password. As such a completely new password is required for the first two expiries; thereafter the first password can be reused.

“Completely new” is defined as having at least fifty percent (50%) of the characters different from the previous password.

Passwords are not needed to access data classified as “Public” or the systems that host this data, as long as these systems do not host data of a higher classification level and so no reuse guidelines need to be set.

Password Protection Guidelines

Passwords are to be treated as confidential information. Under no circumstances is an employee to give, tell, or hint at their password to another person, including IT staff, administrators, superiors, other co-workers, friends, and family members.

Under no circumstances will any member of the organization request a password without the request coming from both a representative of the IT department and the user’s direct manager. Should a request be made that does not conform to this standard, immediately inform both the IT department and your direct manager.

Passwords are not to be transmitted electronically over the unprotected Internet, such as via e-mail. However, passwords may be used to gain remote access to company resources via the company’s Virtual Private Network or SSL-protected Web site.

No employee is to keep an unsecured written record of his or her passwords, either on paper or in an electronic file. If it proves necessary to keep a record of a password, then it must be kept in a controlled access safe if in hardcopy form or in an encrypted file if in electronic form.

Do not use the “Remember Password” feature of applications.

Passwords used to gain access to company systems are not to be used as passwords to access non-company accounts or information. Similarly, passwords used to access personal, non-work related accounts are not to be used to access company accounts.

Each application, system and data point should be protected by a different password where possible. The use of the same password to protect all access is strongly discouraged.

If an employee either knows or suspects that his/her password has been compromised, it must be reported to the IT Department and the password changed immediately. If the minimum aging requirement has not been met for the password, the IT department will reset the minimum aging for the account allowing the user to create a new password.

The IT Department may attempt to crack or guess users' passwords as part of its ongoing security vulnerability auditing process. If a password is cracked or guessed during one of these audits, the user will be required to change his or her password immediately.

Remote Access

It is the responsibility of any employee of AGSL with remote access privileges to ensure that their remote access connection remains as secure as his or her network access within the office. It is imperative that any remote access connection used to conduct AGSL business be utilized appropriately, responsibly, and ethically. Therefore, the following rules must be observed:

General access to the Internet by residential remote users through AGSL's network is permitted. However, both the employee and his/her family members using the Internet for recreational purposes through company networks are not to violate any of AGSL's Internet acceptable use policies.

Employees will use secure remote access procedures. This will be enforced through public/private key encrypted strong passwords in accordance with AGSL's password policy. Employees agree to never disclose their passwords to anyone, particularly to family members if business work is conducted from home.

All remote computer equipment and devices used for business interests, whether personal- or company-owned, must display reasonable physical security measures. Computers will have installed whatever antivirus software deemed necessary by AGSL's COO.

Remote users using public hotspots for wireless Internet access must employ for their devices a company-approved personal firewall, VPN, and any other security measure deemed necessary by the COO. VPNs supplied by the wireless service provider should also be used, but only in conjunction with AGSL's additional security measures.

Hotspot and remote users must disconnect wireless cards when not in use in order to mitigate attacks by hackers, wardrivers, and eavesdroppers.

Users must apply new passwords every business/personal trip where company data is being utilized over a hotspot wireless service, or when a company device is used for personal Web browsing.

Any remote connection (i.e. hotspot, ISDN, frame relay, etc.) that is configured to access AGSL resources must adhere to the authentication requirements of AGSL's COO. In addition, all hardware security configurations (personal or company-owned) must be approved by AGSL's COO.

Employees, contractors, and temporary staff will make no modifications of any kind to the remote access connection without the express approval of AGSL's COO. This includes, but is not limited to, split tunneling, dual homing, non-standard hardware or security configurations, etc.

Employees, contractors, and temporary staff with remote access privileges must ensure that their computers are not connected to any other network while connected to AGSL's network via remote access, with the obvious exception of Internet connectivity.

In order to avoid confusing official company business with personal communications, employees, contractors, and temporary staff with remote access privileges must never use non-company e-mail accounts (e.g. Hotmail, Yahoo, etc.) to conduct AGSL business.

No employee is to use Internet access through company networks via remote connection for the purpose of illegal transactions, harassment, competitor interests, or obscene behavior, in accordance with other existing employee policies.

All remote access connections must include a "time-out" system. In accordance with AGSL's security policies, remote access sessions will time out after 30 minutes of inactivity, and will terminate after 8 hours of continuous connection. Both time-outs will require the user to reconnect and re-authenticate in order to re-enter company networks. Should a remote user's account be inactive for a period of 60 days, access account privileges will be suspended until the COO is notified.

If a personally- or company-owned computer or related equipment used for remote access is damaged, lost, or stolen, the authorized user will be responsible for notifying their manager and AGSL's COO immediately.

The remote access user also agrees to immediately report to their manager and AGSL's COO any incident or suspected incidents of unauthorized access and/or disclosure of company resources, databases, networks, etc.

The remote access user also agrees to and accepts that his or her access and/or connection to AGSL's networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity.

As with in-house computers, this is done in order to identify accounts/computers that may have been compromised by external parties.

AGSL will not reimburse employees for business-related remote access connections made on a pre-approved privately owned ISP service. All submissions for reimbursement must be accompanied by sufficient and appropriate documentation (i.e. original service bill). Employees requesting reimbursement will also be asked to certify in writing prior to reimbursement that they did not use the connection in any way that violates company policy.

Personnel Security

Upon starting work for AGSL employees and third party users will be required to sign appropriate access agreements including non-disclosure, non-compete, conflict of interest, and acceptable usage agreements. These agreements specify the user's intent to abide by the operational and security requirements of AGSL. These agreements will be reviewed on an annual basis and re-signed by information system users at that time.

Should the user of a AGSL information system, whether internal employee or third party user, change working location or system role while in the employ of AGSL, the access and operational privileges of that user will be immediately reviewed and, where required, updated. This review and update will focus equally on eliminating access privileges no longer required as well as providing the net new/enhanced access required of the new functional role. As necessary, AGSL property, temporarily in the possession of the information system user, will be returned.

Should the user of a AGSL information system, whether internal employee or third party user, leave the employ of AGSL, access accounts for all information systems will immediately be suspended. All accounts, even though suspended, will be maintained for a pre-defined period of time to allow for the extraction and retention of necessary information. Thereafter, all accounts shall be permanently deleted. Exit interviews will be conducted and the AGSL will retrieve all AGSL property temporarily in the possession of the information system user.

Security Infrastructure

Boundary network access points will be protected by boundary protection systems (generally a firewall) that monitor and control communications. These systems will be configured to deny communications by rule and allow by exception, to prevent public access to internal networks and to place controls on publicly accessible systems.

Boundary network access points will be protected by monitoring and/or intrusion prevention systems that monitor events, detect attacks, and provide identification of unauthorized information system use. These systems will be configured to monitor both inbound and outbound communications.

All information systems will be protected by malware protection systems where such solutions exist for the information system. At a minimum malware protection will be performed at the network boundary, on e-mail and other communications systems, and on all workstations, servers and other endpoints.

Boundary network access points as well as all information systems will be protected by data protection platforms that monitor, control and restrict the flow of data into and out of systems and into and out of networks. These platforms will include data encryption, session encryption and content filtering.

Refer also to http://labmice.techtarget.com/articles/winxpsecuritychecklist.htm for a Windows XP security best practice checklist (modify where appropriate for application to other operating systems).

System Monitoring and Auditing

Information systems will be configured to record login/logout and all administrator activities into a log file. Additionally, information systems will be configured to notify administrative personnel in the event that inappropriate, unusual and/or suspicious activity is noted. Inappropriate, unusual and/or suspicious activity will be fully investigated by appropriate administrative personnel and findings reported to appropriate security management personnel

Information systems are to be provided with sufficient primary (online) storage to 30 days' worth of log data and sufficient secondary (offline) storage to retain 1 year's worth of data. If primary storage capacity is exceeded, the information system will be configured to overwrite oldest logs. In the event of other logging system failures the information system will be configured to notify the COO.

System logs shall be manually reviewed monthly. Inappropriate, unusual and/or suspicious activity will be fully investigated by appropriate administrative personnel and findings reported to appropriate security management personnel

System logs are considered confidential information. As such all access to system logs and other system audit information requires prior authorization and strict authentication. Further, access to logs or other system audit information will be captured in the logs.

Data Security

Data Types

AGSL deals with two main kinds of data:

1. Company-owned data that relates to such areas as corporate financials, employment records, payroll, [etc.]
2. Private data that is the property of our clients and/or employees, such as social security numbers, credit card information, contact information, [etc.]

Data Classifications

AGSL's data is comprised of 4 classifications of information:

1. Public/Unclassified. This is defined as information that is generally available to anyone within or outside of the company. Access to this data is unrestricted, may already be available and can be distributed as needed. Public/unclassified data includes, but is not limited to, marketing materials, annual reports, corporate financials [and other data as applicable].

   Employees may send or communicate a public/unclassified piece of data with anyone inside or outside of the company.

2. Private. This is defined as corporate information that is to be kept within the company. Access to this data may be limited to specific departments and cannot be distributed outside of the workplace. Private data includes, but is not limited to, work phone directories, organizational charts, company policies [and other data as applicable].

   All information not otherwise classified will be assumed to be Private. Employees may not disclose private data to anyone who is not a current employee of the company.
3. Confidential. This is defined as personal or corporate information that may be considered potentially damaging if released and is only accessible to specific groups [e.g. payroll, HR, etc]. Confidential data includes, but is not limited to, social security numbers, contact information, tax forms, accounting data, security procedures [and other data as applicable]. AGSL considers it a top priority to protect the privacy of our clients and employees. A separate privacy policy [provide link] outlines our commitment to protecting personal data.

Employees may only share confidential data within the department or named distribution list.

4. Secret/Restricted. This is defined as sensitive data which, if leaked, would be harmful to AGSL, its employees, contractors [and other parties as applicable]. Access is limited to authorized personnel and third parties as required. Secret/restricted data includes but is not limited to audit reports, legal documentation, business strategy details [and other data as applicable].

   Secret/restricted data cannot be disclosed by anyone other than the original author, owner or distributor.

It is the responsibility of everyone who works at AGSL to protect our data. Even unintentional abuse of classified data will be considered punishable in accordance with the extent and frequency of the abuse.

IT Support

To lodge an IT support request, please send an email to itsupport@imia.edu.au and include:

- Your name, location and contact phone number
- A description of the hardware of software the support call relates to
- A detailed description of the help you need
- Any other relevant information that may assist.

IT Development

In order to ensure that significant IT development initiatives support organisational objectives, business users of the proposed end product or service of significant IT development initiatives must be involved in the specification and testing of IT development initiatives. The level of involvement in IT development initiatives of business users may vary from project to project, but the plans for involving business end users in initiative specification and testing are to be detailed in the initiative development plan and are to be approved by the Board of Directors.

A “significant” IT initiative is any initiative where the projected total cost is in excess of AUD 20,000.

IT development initiatives must use formal change management processes and a formal project management process that includes methodologies, user participation, quality management and appropriate documentation.

Outsourcing

Check the Accounting policy for the threshold over which development projects must be subject to a competitive tender process.

Performance criteria, milestones and reporting procedures are to be established with the third-party vendor at the outset of the initiative and are to be regularly reviewed for appropriateness and to ensure that the vendor is on track for delivery of the initiative within budgeted costs and timeframes.

Third-party vendors awarded outsourced IT development contracts must use a formal project management process that includes methodologies, user participation, quality management and appropriate documentation.

5. Responsibilities

The following are responsible for the application of this policy:

- COO