INFORMATION SECURITY POLICY MANUAL

External

ISPOM v2 0518

Contents

Responsibilities

The Information Security Officer shall ensure that this policy is up-to-date and relevant, and shall be responsible for this policy on behalf of the Vivio Board.

All of Vivio's staff shall comply with this policy. Specific responsibilities are detailed throughout the policy.

Purpose

This policy sets out Vivio's Information Security Policy.

Scope

This policy addresses all aspects of Vivio's policy for information security. It is supported by other complementary policies, standards, procedures and guidelines. Refer to Information Governance Policy for further information on GDPR compliance and associated processes.

Requirement for Information Security Policy

Information stored and processed by Vivio is a valuable business asset. Without adequate levels of protection of the confidentiality, integrity and availability of information, Vivio will not be able to fulfil its business, legal, regulatory and contractual requirements.

Vivio's (and its customers') information is in many forms including electronic data, removable media e.g. CDs and DVDs, paper, and verbal. All forms of information and supporting systems and networks need to be protected from security threats such as malicious software, unauthorised access, computer misuse, information technology failures, human error, and physical security threats.

For these reasons, Vivio has decided to build its Information Security Policy on ISO 27001 and ISO 27002, the International Standards for information security management, which embrace the following information security requirements:

- Confidentiality – protecting information from unauthorised disclosure;
- Integrity – protecting information from unauthorised modification or deletion;
- Availability – ensuring that information and associated services are available to meet Vivio's business needs.

An Information Security Policy Statement has been published by Vivio's Senior Management Board, which justifies and supports the need for Information Security Policy.

The Information Security Policy Manual (this document) identifies Vivio's policies and associated responsibilities.

The Policy applies to all users that have access to our information (including our customers' information) and associated information processing systems, and applies equally to management, permanent and temporary staff, contractors, partners, suppliers and customers. Non-compliance could lead to staff disciplinary action, or prosecution for legal and contractual breaches.

All managers are directly responsible for implementing the Policy within their business areas, and for adherence by their staff.

The Policy shall be regularly reviewed by Vivio's Information Security Officer to ensure that it continues to meet Vivio's requirements. Reviews shall occur annually or when there are significant changes.

Both the Information Security Policy Statement and Manual are fully supported and have been approved by Vivio's Chief Executive Officer.

Specific Information Security Responsibilities

This Information Security Policy Manual identifies information security responsibilities. Those with responsibilities shall be fully supported by Vivio's Senior Management Board to effectively implement their responsibilities.

This section summarises Vivio's information security roles and responsibilities. Further details of responsibilities are documented within the core Information Security Policy (next section).

Vivio's Senior Management Board

Vivio's Senior Management Board is the ultimate owner of this policy and shall ensure that there are adequate levels of commitment and resources to support policy implementation and compliance.

Vivio's Senior Management Board shall be responsible for providing expertise and guidance to ensure that risks are assessed with corporate risk methodologies that have been selected and approved by Vivio.

Information Security Forum

An Information Security Forum shall regularly meet to provide direction, commitment, resources and support for information security management on behalf of Vivio's Senior Management Board. The Information Security Forum shall facilitate the co-ordination of information security activities by involving and communicating with relevant representatives from different parts of Vivio. Broadly, the Information Security Forum shall consider requirements for policy and its implementation and compliance, and shall address all security initiatives and incidents. The Information Security Forum's terms of reference, including details of its role and members, shall be fully documented.

Information Security Officer

On behalf of Vivio's Senior Management Board, the Information Security Officer (ISO)

shall be responsible for documenting and maintaining this policy in line with Vivio's business and security requirements.

Vivio's ISO shall be responsible for implementing this policy, addressing security breaches and incidents and ensuring overall policy compliance. The ISO's job description shall include detailed responsibilities for information security.

Information Asset Owners

Information Asset Owners are members of staff e.g. Directors, who shall be responsible for the security of Vivio's information assets within their business areas. The responsibilities of Information Asset Owners shall include on-going evaluation and control of risks to information assets under their protection. Information Asset Owners shall ensure that access to information systems under their management is strictly controlled, and shall implement measures to avoid fraud and forgery e.g. using segregation of duties.

Line Managers

All line managers shall be responsible for ensuring that their staff are aware of and comply with this policy. Staff using computer systems and removable media shall be trained in their use before access is granted. Line Managers shall ensure that access to information systems is strictly controlled and that Human Resources, IT Services, Information Asset Owners and Office Management Services (as relevant) are immediately notified when staff leave Vivio or change job functions.

All Users

All users with access to Vivio's information and information processing facilities shall be responsible for information security and ensuring that no breaches of information security result from their actions. Users shall familiarise themselves with this policy and its supporting sub-policies, standards, procedures and guidelines.

IT Services

IT Services shall be responsible for the security of the corporate IT network and all electronic information systems. IT Services shall also be responsible for implementing appropriate IT security standards, controls, procedures and guidelines. As appropriate, IT Services shall be supported by other members of staff, who are responsible for developing, testing and implementing secure IT systems.

Together with the Information Security Officer, IT Services shall be responsible for ensuring that compliance with this policy is regularly reviewed.

Office Management Services

Office Management Services shall be responsible for implementing and maintaining physical and environmental security controls for Vivio's offices. Office Management Services shall also be responsible for assisting IT Services with the implementation of physical security measures such as air conditioning systems.

Human Resources

Human Resources shall be responsible for providing support for human resources security, including responsibilities for pre-employment, during- employment and post-employment security requirements.

Business Continuity Management Team

The Business Continuity Management Team shall be responsible for defining, implementing, testing and maintaining a Vivio-wide business continuity management strategy and plan.

Legal Department

The Legal Department shall be responsible for providing policies, procedures and guidelines to ensure that Vivio complies with its legal, statutory, regulatory and contractual obligations.

The Legal Department shall also be responsible for documenting and maintaining Vivio's Records Retention and Disposal Policy and Schedule, which shall be used to manage the integrity and availability requirements of valuable Vivio information, in line with its legal, regulatory, contractual and business requirements.

Data Protection Officer

Vivio's Data Protection Officer shall have responsibilities for ensuring that Vivio complies with the General Data Protection Regulations. (Refer to Information Governance Policy.)

Internal Organisation

Objective: To manage information security within Vivio

Management Commitment to Information Security

This policy provides evidence of Vivio's intent to actively support information security within Vivio through clear direction, demonstrated commitment, and acknowledged and assigned information security responsibilities. Vivio has appointed specialist groups and roles to address Vivio's security requirements such as the Information Security Forum and an Information Security Officer. Vivio's Senior Management Board shall continue to provide overall direction and approval for information security measures within Vivio.

Information Security Co-ordination

The Specific Information Security Responsibilities section of this policy identifies how information security activities shall be co-ordinated between roles and job functions within different parts of Vivio. The Information Security Forum and the Information Security Officer shall play key roles in ensuring information security co-ordination.

Allocation of Information Security Responsibilities

The Specific Information Security Responsibilities section of this policy summarises information security responsibilities for each role and job function. The remainder of this policy documents detailed responsibilities for information security.

Authorisation Process for Information Processing Facilities

A procedure shall be devised and implemented to ensure that all information processing facilities to be used for storing and processing Vivio's (and its customers') information are formally authorised by IT Services before usage. This shall include use of all new and reconfigured hardware, software and corporate network components. All users shall not use personally owned information processing facilities e.g. Personal Digital Assistants (PDAs) to store and process Vivio's information without formal authorisation from IT Services.

Confidentiality Agreements

All users that have access to Vivio's non-public information and its information processing systems shall sign-up to Vivio's standard confidentiality agreement devised and maintained by Human Resources, before access is granted. This applies equally to management, permanent and temporary staff, and contractors. A confidentiality agreement shall be included within terms and conditions of employment that are issued and signed up to at the start of employment. Confidentiality agreements shall address specific confidentiality requirements, ownership of information, expected duration of the agreement, terms for information to be returned or destroyed at agreement cessation, actions to be taken in case of a breach of the agreement, and the right to audit and monitor activities that involve confidential information.

Contact with Authorities

In order to protect itself from security risks such as criminal damage, fire and flooding, and Internet risks, Vivio shall maintain appropriate contacts with relevant authorities such as the police, the fire brigade, its Internet Service Provider (ISP), telecommunications providers and utilities. Vivio's security incident procedures and business continuity plans shall address requirements for contacting such authorities.

Contact with Special Interest Groups

Vivio shall maintain appropriate contact with external information security specialists to ensure that it is keeping abreast of the latest information security risks and protection measures. In particular, the Information Security Officer and IT Services shall maintain ongoing contact with experts in security threats and vulnerabilities, and security patches and solutions.

Independent Review of Information Security

Vivio's approach to managing information security, including policy implementation, effectiveness and compliance levels, shall be independently reviewed and documented at regular intervals, or when significant changes to the security implementation occur, via an internal audit programme and documented audit procedures. Vivio's Information Security Officer shall be responsible for ensuring that this requirement is fulfilled. The results of these independent audits shall be reviewed by the Information Security Forum and Vivio's Senior Management Board.

External Parties

Objective: To maintain the security of Vivio's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties

Identification of Risks Related to External Parties

A documented risk assessment, and resulting implementation and documentation of secure access controls shall take place for any third party that requires access to Vivio's information and information processing facilities. Standard secure access controls shall be implemented as far as possible. IT Services shall be responsible for these requirements, and, together with the relevant business unit, shall authorise each request for a third party connection to Vivio's information processing facilities before third party access is granted. Each connection shall be terminated as soon as possible e.g. at the end of the third party access session, and (if appropriate) automatically after a specified time e.g. at a set time of the day. Third parties shall not be able to re-establish the connection once it is terminated without IT Services' intervention. IT Services shall ensure that third party access privileges are appropriately restricted and monitored. Third parties include all customers, partners and suppliers e.g. of hardware and software solutions.

Addressing Security When Dealing with Customers and Business Partners

Policy under the Identification of Risks Related to External Parties section of this policy shall also apply when granting Vivio's customers and business partners with access to our information and information processing facilities.

Addressing Security in Third Party Agreements

Information security and relevant service delivery requirements shall be incorporated within formal agreements for any third party e.g. service provider, customer and business partner that accesses, develops or supports Vivio's information and information processing facilities. This shall also include third parties providing Vivio with outsourcing or facilities management arrangements (if relevant), where Vivio's information and software is accessible to such third parties. All relevant contracts with third parties shall draw attention to compliance with this policy. Third party agreements shall address specific confidentiality requirements, ownership of information, hardware and software (as relevant), legal obligations e.g. data protection and copyright, expected duration of the agreement, terms for information to be returned or destroyed at agreement cessation, actions to be taken in case of a breach of the agreement, and the right to audit and monitor activities that involve Vivio's information and information processing facilities.

Responsibility for Assets

Objective: To achieve and maintain appropriate protection of Vivio's assets

Inventory of Assets

Vivio shall implement and maintain records of its information assets within a Retention and Disposal Policy and Schedule. This document shall identify all valuable information assets that belong to Vivio, and shall be maintained by Vivio's Legal Department. Information Asset Owners shall regularly notify the Legal Department of any required additions or changes to the Records Schedule.

Inventories shall be created and maintained of all IT assets purchased and used by Vivio i.e. all hardware, software and telecommunications equipment. Inventories shall include up-to-date details of asset owners, users and locations, as well as asset serial numbers and purchase dates. A procedure shall be established to ensure that the inventory register is kept up-to-date and audited on a regular basis. Software inventories shall be maintained to ensure that license conditions are followed. IT Services shall be responsible for maintaining a central register of IT asset inventories.

Ownership of Assets

As stated in the Specific Information Security Responsibilities section of this policy, Information Asset Owners e.g. Directors shall be responsible for the security of Vivio's information assets within their business areas. IT Services shall be the owner of all IT assets that belong to Vivio.

Acceptable Use of Assets

Vivio shall document and implement requirements for the acceptable use of information and information processing facilities. The requirements shall be regularly reviewed and maintained to ensure that they continue to meet Vivio's needs. All users shall be responsible for complying with Vivio's requirements for the acceptable use of assets. In support of this policy, detailed requirements for the acceptable use of IT assets are documented in Vivio's Information Security User Guide as well as its E-mail, Phone and Internet Usage Policy, both of which shall be formally issued to all users.

Information Classification

Objective: To ensure that information receives an appropriate level of protection

Classification Guidelines

Vivio shall devise and implement information classification, labelling and handling procedures. The procedures shall identify protective marking classes

for categorising Vivio's information according to its sensitivity, potential impacts upon unauthorised disclosure, and the access restrictions that apply. Information Asset Owners shall classify and label information for which they are responsible according to the procedures.

Information Labelling and Handling

The information classification, labelling and handling procedures shall document security requirements within each information class for copying, storing, processing, transmitting and disposing of information in any format e.g. electronic, media and paper. All users of Vivio's (and its customers') information shall ensure that it is securely handled according to its classification label in line with the procedures.

Human Resources Security

Prior to Employment Objective: To ensure employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities

Roles and Responsibilities

Security roles and responsibilities identified in this policy shall also be documented in individual job descriptions as appropriate. In particular, this shall apply to employees, contractors and third parties with greater responsibilities for information security as stated in the Specific Information Security Responsibilities section (above) e.g. the Information Security Officer, and IT Services' system and database administrators. This shall be the responsibility of Human Resources and relevant Line Managers.

Screening

All permanent and temporary staff shall be recruited using Vivio's standard recruitment procedures which shall be documented and maintained by Human Resources. These shall include appropriate background verification checks which shall be carried out before making any appointment. Checks shall be in accordance with relevant laws and appropriate to the role and information being accessed. As a minimum, checks shall include two references, an identification check (e.g. production of passport, birth certificate or driving licence) and confirmation of qualifications. For posts processing very sensitive information, additional vetting checks may be made to ensure employee suitability e.g. Criminal Records Bureau (CRB) and / or credit history checks. Human Resources shall be informed of all intentions to recruit contracting staff to ensure that contractors are subject to suitable screening e.g. via a formal agreement between Vivio and a contractor agency.

Terms and Conditions of Employment

Human Resources shall ensure that terms and conditions of employment state responsibilities for information security i.e. the requirement to comply with this information security policy. These shall be signed up to by employees before employment commences. See Confidentiality Agreements and Roles and Responsibilities above for related information.

During Employment

Objective: To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support this policy in the course of their normal work, and to reduce the risk of human error

Management Responsibilities

Management shall ensure that employees, contractors and third party users (for whom they are responsible) are adequately informed of their responsibilities to adhere to this policy.

Information Security Awareness, Education and Training

All users shall be made aware of and shall understand this policy (and supporting standards, procedures and guidelines) before access is granted to Vivio's information. Regular reminders, and awareness and education of policy changes shall also be provided. Line Managers shall be responsible for ensuring that their staff are properly trained, whilst Vivio's Information Security Forum and Information Security Officer shall be responsible for ensuring that an on-going training and awareness programme is fully implemented.

Disciplinary Process

Human Resources shall be responsible for documenting and maintaining a Disciplinary Procedure. This procedure shall apply to all permanent and temporary staff, and disciplinary action including dismissal may be taken in the event of a breach of this policy.

Termination or Change of Employment

Objective: To ensure that employees, contractors and third party users exit Vivio or change employment in an orderly manner

Termination Responsibilities

Line Managers and Human Resources shall be responsible for ensuring that employees and contractors exit Vivio or change employment in an orderly manner. Similar responsibilities for third parties shall lie with those who are responsible for employing third parties. Duties shall include implementation of a documented procedure (and completion of a job termination form) to provide all relevant parties (including Information Asset Owners, IT and Office Management Services) with timely information concerning all employees, contractors and third parties who leave Vivio or change jobs within Vivio.

Return of Assets

Vivio shall ensure that all employees, contractors and third party users that no longer require access to Vivio's information and information processing Office Management Services shall return all of Vivio's assets e.g. laptops in a timely and orderly manner. The procedure identified under Termination Responsibilities above shall include responsibilities (and the completion of a form) for the return of assets. All users shall facilitate the timely return of Vivio's assets that have been given to them during their employment.

Removal of Access Rights

Vivio shall ensure that all employees, contractors and third party users that no longer require access to Vivio's information and information processing Office Management Services shall no longer be able to access Vivio's non-public information and information processing Office Management Services. The procedure identified under Termination Responsibilities above shall include responsibilities (and the completion of a form) for the removal of access rights. In addition, IT shall check once a quarter for unused user accounts, and disable them subject to approval from relevant Line Managers.

Physical and Environmental Security

Secure Areas

Objective: To prevent unauthorised physical access, damage and interference to Vivio's premises and information

Physical Security Perimeter

For Vivio's offices, security perimeters shall be defined by the use of physical access controls, and secure, lockable windows and doors. Fire escapes shall be controlled to avoid unauthorised access. Office Management Services shall be responsible for the provision of adequate physical security perimeters, and defining and implementing relevant procedures. All users that have authorised access to Vivio's offices shall protect against access by unauthorised persons, including tailgating.

Physical Entry Controls

Physical entry controls shall be defined by the authorised use of physical access controls i.e. use of secured non-electronic access keys. All visitors to Vivio's offices shall report to the reception area, sign in to the visitor's book, always wear a visitor's badge for identification, be escorted at all times whilst within Vivio's offices, and sign-out of the visitor's book upon departure. Staff shall challenge any unrecognised and unescorted person within Vivio's offices. In addition, Vivio shall use CCTV to monitor entry points into Vivio's offices.

Securing Offices, Rooms and Office Management Services

Secure, lockable rooms shall be used to protect functions with special security requirements e.g. the computer room. Secure, lockable cabinets shall be used to store all sensitive information whilst left unattended e.g. sensitive information belonging to Human Resources and IT, as well as unattended laptops, Personal Digital Assistants (PDAs), and computer media. Computer servers and core network equipment are further considered below (see Equipment Siting and Protection).

Protecting Against External and Environmental Threats

Vivio's offices shall be adequately protected from physical security threats such as fire and flooding. Office Management Services shall be responsible for the provision of adequate site controls e.g. timely contact with the Emergency Services, and defining and implementing relevant procedures e.g. building evacuation, and dealing with suspicious packages. All users shall ensure that they are familiar with Vivio's controls and procedures. IT shall address risks associated with critical computing and networking equipment. The Business Continuity Management Team shall be responsible for defining and implementing a Vivio-wide business continuity management strategy and plan that include consideration of external and environmental threats.

Working in Secure Areas

Vivio has a Clear Desk and Clear Screen Policy (see below), which shall be implemented by all users. Users shall take account of Vivio's Information Classification requirements (see above). In addition, food and drink shall not be taken into the computer room(s).

Public Access, Delivery and Loading Areas

All deliveries shall be made to reception. External delivery and collections people shall not enter Vivio's offices unless escorted. All users who are responsible for collecting deliveries shall ensure that they are inspected for tampering and damage, and signed-for upon arrival, and are immediately moved to a more secure area.

Equipment Security

Objective: To prevent loss, damage, theft or compromise of assets and interruption to Vivio's activities

Equipment Siting and Protection

IT shall be responsible for IT equipment siting and protection. All computer servers and core network equipment shall be located in secure computer and communication rooms with strict access controls over and above those used to access other areas within Vivio's offices. The computer and communications rooms shall be locked when IT' staff members are not present. To prevent equipment overheating, they shall have adequate air conditioning, which shall be properly maintained according to the manufacturer's standards.

Supporting Utilities

Vivio shall ensure adequate protection against electrical power failures and disruptions. IT shall be responsible for implementing agreed contingency arrangements for IT equipment in line with Vivio's business continuity plans. Critical computer and network equipment shall be fitted with Uninterruptible Power Supply (UPS) technology, which shall (as a minimum) enable controlled system shutdowns in the event of a power failure.

Cabling Security

Vivio shall ensure adequate protection against damage or interference of power and telecommunications cabling that carries data or supports information services. Office Management Services shall be responsible for the security of Vivio's core power and telecommunications cabling systems within its offices, whilst IT shall be responsible for all other cabling that interfaces with computing and network equipment. In all cases, IT industry best practice standards shall be implemented. All core cabling shall be in conduits if surface mounted, otherwise within the framework of the building, and not accessible to unauthorised people. Power cables shall be segregated from communications cables to prevent interference. Colour coded cabling and equipment labelling shall be used to minimise human errors.

Equipment Maintenance

All equipment used to support the storage and processing of information shall be adequately maintained according to manufacturers' maintenance schedules. All IT equipment maintenance shall be formally authorised and

managed by IT. Computer and network equipment shall be covered by warranties or third party maintenance agreements. Wherever possible, new equipment shall be purchased with a three years' warranty agreement. Only authorised personnel shall carry out repairs and service equipment. Documented records of all equipment faults and maintenance shall be maintained.

Security of Equipment Off-Premises

All authorised users shall be responsible for protecting off-site IT equipment (that belongs to Vivio) from physical security threats. Equipment taken off-site shall be locked away and kept out of sight when left unattended. Users shall ensure that unauthorised persons are not able to view Vivio's information on display screens, and shall protect access to unattended equipment by use of an enforced password (by simultaneously pressing the <Ctrl> <Alt> <Delete> keys and selecting 'Lock Computer'). Detailed advice on how to protect equipment whilst off-premises, including at home and whilst travelling, is provided in Vivio's Mobile and Home Worker Guidelines. Users shall also ensure that off-site information (that belongs to Vivio) is securely handled in line with Vivio's Information Classification requirements (see above).

Secure Disposal or Re-use of Equipment

All of Vivio's information and software shall be securely wiped (removed and overwritten) from IT equipment before its disposal or re-use (the latter as appropriate). All equipment disposal and re-use shall be formally authorised and managed by IT, who shall devise appropriate standards and procedures.

Removal of Property

All of Vivio's IT equipment and software shall only be taken off-site following formal authorisation by IT, whilst Vivio's information shall only be taken off-site following formal authorisation from the relevant Information System Owner or Line Manager. All IT equipment (and software) taken off-site shall be signed for by the person taking the equipment to acknowledge responsibility for its welfare. IT shall countersign to authorise the loan. When no longer needed, all IT equipment (and software) shall be returned to IT and signed in by the borrower and IT staff. Upon return, equipment and software shall be immediately moved to a secure storage area.

Communications and Operations Management

Operational Procedures and Responsibilities

Objective: To ensure the correct and secure operation of information processing Office Management Services

Documented Operating Procedures

Documented operating procedures for information systems shall be up-to-date and regularly maintained by relevant Information Asset Owners, Line Managers and IT to enable continuous, error-free and secure processing of information systems. Procedures shall include build instructions for IT computing and networking equipment, including software configurations. Documentation shall adequately cover error and exception handling requirements, and be comprehensive enough to ensure that Vivio's knowledge and expertise is maintained in the event of unexpected staff shortages and losses. Regular, formal reviews of documented operating procedures shall be scheduled to ensure that they remain up-to-date. Up-to-date documented operating procedures shall be distributed to all users who need them to perform their

job functions. Copies of relevant procedures shall also be securely stored off-site for business continuity and disaster recovery purposes.

Change Management

Change management procedures shall be implemented for all significant changes to information processing systems and related documentation. All such changes shall be initially assessed for business and security impacts, formally planned and communicated to those with vested interests, documented, tested and approved, and contingency measures shall be available in case of failure to correctly implement the changes. IT shall be responsible for IT change management, including changes to the network infrastructure and information systems, hardware and software, and related documentation.

Segregation of Duties

To manage the risks of fraud, unauthorised activity, misuse and human error, Vivio shall segregate the duties of its officers where feasible. In particular, for activities and transactions of a very critical and sensitive nature, e.g. financial transactions, Vivio shall ensure that implementation, approval and auditing duties are appropriately segregated. Information Asset Owners and Line Managers shall be responsible for segregating duties in line with Vivio's business and security requirements. IT shall ensure that 'IT administrator' roles are restricted as far as possible, and are regularly monitored and audited. Information system access shall be logged and monitored, especially access involving 'higher' privileges.

Separation of Development, Test and Operational Office Management Services

As necessary and appropriate, IT shall ensure that IT development, test and operational Office Management Services are adequately separated to reduce the risks of unauthorised access and unauthorised changes to the operational environment.

Third Party Service Delivery Management

Objective: To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements

Service Delivery

All third party agreements shall be subject to regular review. Those responsible for third parties, e.g. IT and Information Asset Owners, shall ensure that third parties implement and maintain appropriate levels of information security and service delivery in line with third party agreements. See related policy on Addressing Security in Third Party Agreements above.

Monitoring and Review of Third Party Services

All those with responsibility for managing third parties e.g. IT and Information Asset Owners, shall regularly assess whether third parties are honouring their agreements using formal procedures.

Managing Changes to Third Party Services

Changes to the provision of third party services, including information security procedures and controls, shall be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks. This shall be implemented by those with responsibility for managing third parties.

System Planning and Acceptance

Objective: To minimise the risks of systems failures

Capacity Management

Information processing and storage capacity requirements shall be understood prior to operational implementation of new or changing information systems, including networking capacity requirements. Capacity monitoring shall take place to identify poor performance of or disruption to information processing Office Management Services. Information Asset Owners and IT shall be responsible for identifying new or changing business requirements for capacity management. IT shall be responsible for implementing and maintaining capacities that meet these requirements. Formal procedures and controls shall be used for identifying, implementing and monitoring capacity requirements.

System Acceptance

Prior to implementing all significant information processing changes into operations, there shall be the establishment of acceptance criteria, test plans, test results, and formal acceptance and approval of the changes. Necessary security checks shall be accounted for. Information Asset Owners shall be responsible for user acceptance testing and sign-off, whilst IT shall be responsible for IT acceptance testing and sign-off e.g. testing recovery from computer failures.

Protection Against Malicious and Mobile Code

Objective: To protect the integrity of software and information

Controls Against Malicious Code

Vivio shall ensure that it has adequate technical and procedural controls in place to protect its information and information processing Office Management Services from malicious code attacks e.g. viruses and spyware. IT shall be responsible for implementing appropriate malicious code detection, prevention and recovery controls. All computers (unless deemed unnecessary
e.g. UNIX based computers) and Internet and e-mail gateways (as appropriate) shall be protected by reputable, up-to-date anti-virus and anti- spyware software. As appropriate, all newly acquired software shall be virus checked prior to its use. Detailed advice on how users shall protect against malicious code is provided in Vivio's Information Security User Guide, as well as its E-mail, Phone and Internet Usage Policy. All users shall be responsible for implementing Vivio's policy and guidelines. Users shall report any detected or suspected malicious code immediately to IT and the Information Security Officer, and shall not install any unauthorised software on Vivio's IT equipment.

Controls Against Mobile Code

Mobile code is software that is transmitted across a network, e.g. the Internet, from a remote source to a local system and is then executed on that local system, often without explicit action on the part of the user. The local system could be a personal computer (PC), laptop, personal digital assistant (PDA) or mobile phone. Mobile code could contain malicious code. IT shall ensure that by default, mobile code is unable to execute on Vivio's information processing systems. IT shall authorise all use of mobile code, and in such cases, security awareness training shall be given to relevant staff.

Back-up

Objective: To maintain the integrity and availability of information and information processing Office Management Services

Information Back-up

Back-up and recovery procedures and technology shall be implemented to protect Vivio from losses or corruption of information and software e.g. due to unauthorised changes to information and software, technical failures, viruses and fire. Regular recovery tests using back-ups shall be performed by IT to ensure that a 'business as usual' status can be resumed as quickly as possible following a security incident occurrence. Information Asset Owners shall be responsible for identifying business requirements for back-up and recovery controls (including legal, regulatory and contractual requirements for data retention), whilst IT shall be responsible for implementing suitable back-up and recovery controls and procedures. The successful completion of all back-ups shall be confirmed as soon as possible. Storage of back-ups shall be geographically separate from the backed-up information systems to protect against building loss. All users shall be responsible for ensuring that all changes to information stored on local client devices such as laptops undergo regular

back-ups. It is recommended that such information shall always be copied and stored onto appropriate Vivio servers to ensure that regular back-ups are taken.

Network Security Management

Objective: To ensure the protection of information in networks and the protection of the supporting infrastructure

Network Controls

Controls shall be implemented to achieve and maintain security in Vivio's networks e.g. use of secure firewalls, routers and switches, authentication and access controls, encryption, and logging and monitoring of access. Special controls shall be established to safeguard the confidentiality and integrity of data passing over public or wireless networks e.g. use of authentication and encryption. IT shall be responsible for network security. The requirement for network access control is further addressed within Network Access Control below.

Security of Network Services

Service standards covering the operation of network services shall be drawn up and agreed with users, and regularly reviewed. IT shall be responsible for network service delivery and network security.

Media Handling

Objective: To prevent unauthorised disclosure, modification, removal or destruction of assets, and interruption to business activities

Management of Removable Media

Care shall be taken to protect all removable media (removable disks, tapes, CDs, DVDs, and USB devices e.g. memory sticks and flash drives) and hardcopy documentation containing Vivio's information. Measures shall be taken to ensure secure storage, transit, copying, reuse and disposal of media and hardcopy documentation. Manufacturers' guidelines shall be applied for the protection of media. Users shall ensure that removable media and hardcopy documentation are securely handled in line with Vivio's Information Classification requirements (see above). Depending on the information classification, and when necessary and practical, authorisation from a user's Line Manager shall be required before media and hardcopy documentation are removed from Vivio's offices, and a record of such removals shall be kept by the Line Manager in order to maintain an audit trail. Information stored on removable media that needs to be available longer than the media lifetime shall also be stored elsewhere to avoid information loss due to media deterioration.

Disposal of Media

Removable media and hardcopy documentation shall be securely disposed of when no longer required, in line with Vivio's Information Classification requirements. Users shall seek advice from IT where necessary. All removable media containing Vivio's non-public information shall be securely wiped (data shall be removed or overwritten) before disposal, however if this is not possible, the media shall be destroyed.

Information Handling Procedures

To protect Vivio's information from unauthorised disclosure or misuse, information stored on removable media and in hardcopy documentation shall be securely handled in line with Vivio's Information Classification requirements.

Security of System Documentation

To protect against unauthorised access, system documentation stored on removable media and in hardcopy format shall be securely handled in line with Vivio's Information Classification requirements.

Exchange of Information

Objective: To maintain the security of information and software exchanged within Vivio and with any external entity

Information Exchange Policies and Procedures

Information exchange requirements shall be defined in Vivio's Information Classification requirements (see above), as well as Vivio's E-mail, Phone and Internet Usage Policy. All users shall comply with these requirements.

Exchange Agreements

Where necessary, agreements or protocols shall be established for the exchange of information and software between Vivio and relevant external parties e.g. customers and suppliers. Information Asset Owners shall be responsible for managing such agreements and protocols.

Physical Media in Transit

To protect against unauthorised access, misuse or corruption during transportation, information stored on removable media and in hardcopy documentation shall be securely handled in line with Vivio's Information Classification requirements (see above), e.g. by use of appropriate packaging, recorded delivery, and reputable couriers. All users shall comply with these requirements.

Electronic Messaging and Secure Internet Access

Procedures and controls shall exist to manage e-mail and Internet access to protect Vivio from security threats such as viruses, unsolicited e-mails, fraud, unauthorised content and breaches of legislation e.g. computer misuse and copyright legislation. Legally acceptable controls shall be implemented to block and content check e-mails and Internet access. IT shall be responsible for implementing secure e-mail and Internet access controls, and for maintaining the required availability levels of these systems. All users shall be responsible for complying with Vivio's E-mail, Phone and Internet Usage Policy. To protect against unauthorised access to confidential information within e- mails, information shall be securely handled in line with Vivio's Information Classification requirements (see above).

Business Information Systems - Information Security in Conversations and with the Use of Telephones, Facsimiles, Printers, Scanners and Recording Equipment

All users shall take due care when discussing sensitive information in conversations on Vivio's premises and anywhere else, to protect the interests of Vivio and its data subjects e.g. employees and customers. Due care shall be taken when using telephones, voicemail, answering machines, facsimiles, printers, scanners and recording equipment (e.g. photographic, video and audio equipment) to ensure protection of Vivio's information. Users shall comply with Vivio's Data Protection procedures, and Vivio's Information Classification requirements (see above), and follow detailed advice within the Information Security User Guide.

Electronic Commerce Services

Objective: To ensure the security of electronic commerce services, and their secure use

Electronic Commerce

Information involved in the provision of Vivio's services over public networks, e.g. Vivio's customers' payment cardholder data, shall be protected from fraudulent activity, and unauthorised disclosure and modification. Adequate controls shall be implemented such as secure authentication, encryption, access controls and access logging and auditing. Relevant Information Asset Owners and IT shall be responsible for ensuring that adequate controls are in place.

On-line Transactions

Information involved in on-line transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorised duplication or replay. Policy detailed under Electronic Commerce above also applies to 'On-line Transactions'.

Publicly Available Information

Vivio shall protect its web services and the integrity of publicly available electronic information from security threats such as viruses and unauthorised modification. This includes the need for secure authentication, user access management and secure software configuration. Vivio's web services shall offer availability levels to meet the business requirements of Vivio and its customers.

Web-based Vivio information shall be maintained and up-to-date to meet its legal and business requirements. Information Owners shall be responsible for maintaining up-to-date and relevant information and shall authorise the publication of all Vivio information relevant to their areas, whilst IT shall be responsible for implementing and maintaining appropriate procedures and controls to protect publicly available electronic information.

Monitoring

Objective: To detect unauthorised information processing activities

Audit Logging

Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period (e.g. one year minimum for access to payment card data) to assist in future investigations and access control monitoring. Vivio shall implement standards and procedures for audit logging of network access, operating system access, and applications and information access, and shall identify events and details that need to be captured in audit logs. Information Asset Owners shall be responsible for audit logging requirements for business information systems (applications), whilst IT shall be responsible for audit logging requirements for the IT network and security infrastructure, user 'network' accounts, server and client operating systems, and corporate systems such as e-mail and Internet access. Responsibilities include identifying and implementing audit log retention and archiving needs to comply with legal, regulatory, contractual and evidence gathering requirements.

Monitoring System Use

Procedures for monitoring use of information processing Office Management Services shall be established, and the results of the monitoring activities reviewed regularly (e.g. daily monitoring of access to customers' cardholder data is required). Vivio, within its legal rights, shall monitor day-to-day access and use of its information processing Office Management Services to ensure adequate protection from security threats, and where necessary, shall collect evidence of misuse and unauthorised activities. Information Asset Owners shall be responsible for monitoring access of business information systems (applications), whilst IT shall be responsible for monitoring access of the network and security infrastructure, user 'network' accounts, server and client operating systems, and corporate systems such as e-mail and Internet access. Suitable technology and adequate staff resources shall be identified and implemented to support this policy.

Protection of Log Information

Logging Office Management Services and log information shall be protected against tampering and unauthorised access using appropriate controls e.g. authentication and access controls. Information Asset Owners and IT shall ensure that access to log information is restricted on a 'need-to-know' basis, and only to 'trusted' staff.

Administrator and Operator Logs

System and database administrator activities shall be logged. This shall be the responsibility of Information Asset Owners and IT. Where necessary, logs of administrator activity shall be immediately copied to a secure area that is only accessible to the Information Security Officer, to protect against any tampering of evidence of access.

Fault Logging

Fault logging procedures and controls shall be used to address faults in information processing systems, with the ability to record fault details, the fault 'reporter', dates and times, on-going fault status and corrective actions, and to assist with the analysis of fault types, frequencies, impacts and costs. IT shall be responsible for implementing the fault logging procedures and controls, and regularly reviewing faults to ensure that all faults have been satisfactorily resolved, and to identify ways of improvement. All users shall comply with requirements for reporting faults to IT as soon as possible.

Clock Synchronisation

IT shall be responsible for ensuring that the computer clocks of all information processing Office Management Services are synchronised using an accurate, reputable time source.

Access Control

Business Requirement for Access Control Objective: To control access to information

Access Control Policy

All access to Vivio's information (including its customers' information) and information processing Office Management Services shall be restricted on a 'need-to-know' basis. As far as possible, each user shall access information using a unique user ID and password. This policy shall be enforced by Information Asset Owners and IT.

User Access Management Objective: To ensure authorised user access and to prevent unauthorised access to information systems

User Registration

Formal procedures shall exist for the registration and de-registration of all user accounts, and the granting of access to Vivio's network, information systems, and Internet and e-mail Office Management Services. Records of user registration, de-registration and access privileges shall be maintained. Where possible, each user shall be given a unique user account only accessible to the individual user, to enable full tracking of user actions. A user shall not share any user (network or application) account with another user without prior authorisation from IT and the user's Line Manager. Line Managers shall be responsible for informing IT of all registration, access and de-registration requirements as soon as possible, and IT shall be responsible for implementing these requirements. De-registration procedures are addressed within Termination or Change of Employment above.

Privilege Management

Access privileges shall be limited to a level that ensures that each user is able to perform their job function (but no further functions). They shall be implemented via the procedures detailed in User Registration above.

User Password Management

Information Asset Owners shall be responsible for ensuring that secure authentication methods such as use of user IDs and strong passwords are used to access business information systems (applications). IT shall ensure that secure authentication methods are used to access the IT network and security infrastructure, server and client operating systems, and corporate systems such as Internet and e-mail. This includes secure authentication of all 'IT administrator' access, and may involve use of more secure forms of authentication e.g. two factor authentication, such as use of hardware tokens. Two factor authentication is required for Internet based access to Vivio's payment card data environment. Temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced

to change immediately upon the next account log-on. Passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption) and protected from unauthorised access. Whenever feasible, IT and Information Asset Owners shall implement password controls that include enforcement of password strength (via length and format), regular password changes, inability to re-use previously used passwords, and user account lockout after a small number of bad password attempts. The following guidelines shall be followed, based on the Payment Card Industry Data Security Standard (PCI DSS).

Minimum Password Length	7 characters
Password Format	Must contain: ▪ A mixture of alphabetic and numeric characters ▪ A mixture of uppercase and lowercase characters ▪ Optional use of special characters e.g. @%#?
Maximum Password Lifetime	90 days
Password History	Last 4 passwords cannot be re-used
Account Lockout Threshold	6 successive incorrect log-on attempts

Review of User Access Rights

User access rights shall be subject to formal review on a regular basis. Information Asset Owners and IT shall undertake quarterly checks to verify that user access rights are being properly managed, and unnecessary rights shall be removed. Special access privileges (including 'IT administrator' access) shall also be reviewed quarterly.

User Responsibilities

Objective: To prevent unauthorised user access, and compromise or theft of information and information processing Office Management Services

Password Use

Users shall be responsible for keeping their passwords confidential at all times, and shall not disclose passwords to anyone, including IT staff and their Line Managers. Written down passwords shall be discouraged, unless documentation is completely inaccessible to other persons. Weak passwords, as defined in Vivio's Information Security User Guide, shall not be used. Users shall choose password lengths and formats by following the guidelines in User Password Management above.

Unattended User Equipment

Users shall protect their Vivio IT equipment from unauthorised access when left unattended by simultaneously pressing the <Ctrl> <Alt> <Delete> keys and selecting 'Lock Computer'. IT shall implement standard computer screen

locking mechanisms that disable access after a defined length of user inactivity i.e. 15 minutes or less time.

Clear Desk and Clear Screen Policy

A 'Clear Screen Policy' shall be implemented by use of the controls listed under Unattended User Equipment above. In addition, users shall ensure that all valuable and sensitive mobile equipment e.g. laptops, computer media and hardcopy information are removed from their desks when left unattended, and are appropriately stored in locked areas or Office Management Services e.g. locked cabinets, and that access to 'container' keys is properly controlled. Users shall comply with Vivio's Information Classification requirements (see above).

Network Access Control

Objective: To prevent unauthorised access to network services

Policy on Use of Network Services

Users shall only be provided with access to Vivio's network services that they have been specifically authorised to use, in line with the User Registration policy above. Access to Vivio's network services shall be strictly managed by IT based on business requirements. Only IT (and suitable personnel appointed by them) shall have privileges to access and change network configurations.

User Authentication for External Connections

IT, together with relevant Information Asset Owners and Line Managers shall authorise all external connections to Vivio's network. Appropriate authentication methods shall be used to control access to Vivio's network by remote users. By default, all remote users including Vivio's employees e.g. 'IT administrators' and third parties shall use a secure encrypted path over the Internet e.g. Virtual Private Network (VPN) or Secure Sockets Layer (SSL). Where necessary (e.g. for access to Vivio's payment card data environment), remote users shall also use two factor authentication such as a security token or individual SSL certificate. The use of modems and dial-in technology shall be strictly controlled and discouraged by IT. Requirements for third party access are further defined in Identification of Risks Related to External Parties above.

Equipment Identification in Networks

Where necessary, and in addition to user authentication, Vivio may also authenticate equipment connections (using MAC addresses and IP addresses) to the network from specific locations and equipment e.g. for point-to-point connections, or for identification of wireless client devices when accessing a Vivio wireless network. IT shall be responsible for identifying the need for equipment identification in networks.

Remote Diagnostic and Configuration Port Protection

IT shall implement controls to restrict remote access to Vivio's network services and information systems based upon business needs. By default, access to Vivio's network, each information system, each application and each network service e.g. use of telnet or ftp shall be blocked. IT shall justify and authorise access to any network service, and ensure that access is controlled by secure means.

Segregation in Networks

Vivio's network shall be segmented to protect sensitive information systems belonging to Vivio and its customers from unauthorised access via Internet, wireless and internal network based access. Secure firewalls (and other controls such as Virtual Private Networks (VPNs) and two factor authentication) shall be used to control remote access across the Internet. IT shall also use other appropriate technologies e.g. secure firewalls, Virtual LANs (VLANs) and routers, to segregate the internal network where necessary.

Network Connection Control

IT shall ensure that secure network connection controls are in place, i.e. firewalls and routers, between Vivio's and any other organisation's network, including the Internet. The controls shall be configured to restrict access in line with Vivio's business and security requirements.

Network Routing Control

IT shall ensure that network routing controls are implemented so that computer connections and information flows are restricted in line with Vivio's business and security requirements.

Operating System Access Control

Objective: To prevent unauthorised access to operating systems

Secure Log-on Procedures

Operating system access control applies to all computers that have an operating system e.g. servers, PCs, and laptops. IT shall ensure that log-on procedures are secure and do not provide unnecessary information that could enable unauthorised access e.g. provide clues about valid user IDs or the operating system version (and therefore its vulnerabilities). Operating system and network account log-on procedures shall also include an enforced user acknowledgement to comply with the Computer Misuse Act, 1990. All successful and unsuccessful log-on attempts shall be logged and monitored.

User Identification and Authentication

IT shall ensure that, as far as possible, all operating system users have a unique user ID for their individual use only, so that activities can be traced to the individual responsible. This shall include use of unique user IDs for system administrator access too.The default authentication technique shall involve use of strong passwords (by following the guidelines in User Password Management above), however, there may be justification for use of stronger authentication techniques e.g. remote system administration access that uses two-factor authentication (such as hardware tokens) is required for access to Vivio's payment card data environment.

Password Management System

Operating system access shall be protected by use of secure password management, by following the guidelines provided in User Password Management above.

Use of System Utilities

IT shall ensure that operating system utility programs that might be capable of overriding system and application controls are restricted by use of appropriate authentication and access controls (or completely removed).

Session Time-out

By default, the controls listed in Clear Desk and Clear Screen Policy (above) apply. In addition, Information Asset Owners and IT shall consider implementation of session (e.g. database transaction) time-outs after a defined period of inactivity where applicable i.e. where the requirement is justified by risk to information security.

Limitation of Connection Time

Information Asset Owners and IT shall consider implementation of connection time limitations where applicable (where the requirement is justified by risk to information security). For example, third party support access shall be limited to specific times according to Vivio's requirements.

Application and Information Access Control

Objective: To prevent unauthorised access to information held in application systems

Information Access Restriction

Access to Vivio's electronic information (including information stored in applications, file servers, e-mail systems, and web systems) and application functions shall be strictly controlled by IT and Information Asset Owners. This shall include use of unique user IDs to enable accountability for user actions, restricted privileges based on job functions, and secure password management by applying policy in User Access Management above. Access to information shall be controlled in line with Vivio's Information Classification requirements above.

Sensitive System Isolation

IT and Information Asset Owners shall ensure that, where relevant, sensitive information systems have a dedicated (isolated) computing environment i.e. by use of separate computers or secure drive partitions that ensure that users of other Vivio systems are not able to access the more sensitive systems in an unauthorised way.

Mobile Computing and Home Working

Objective: To ensure information security when using mobile computing and home working Office Management Services

Mobile Computing and Communications

Mobile workers include all users who use and access Vivio's (and its customers') information and information processing Office Management Services whilst not located on a Vivio site e.g. workers who are located at home, in hotels and conferences, and workers who are travelling. Mobile workers shall be responsible for the physical protection of Vivio's information processing Office Management Services (e.g. laptops) in their possession as defined in Security of Equipment Off-Premises above. IT shall be responsible for implementing controls for secure remote access to Vivio's network, protection against malicious software attacks e.g. viruses, secure personal firewalls, and secure Internet access. Mobile workers shall be responsible for ensuring that back-ups of Vivio's information stored on mobile devices are performed at regular intervals to avoid loss or corruption of information. Mobile workers shall also be responsible for following advice provided in Vivio's Mobile and Home Worker Guidelines.

Home Working

Home workers are users who have been authorised to use Vivio's (and its customers') information and information processing Office Management Services whilst based at home. All home workers shall comply with policy defined under Mobile Computing and Communications above.

Information Systems Acquisition, Development and Maintenance

Security Requirements of Information Systems

Objective: To ensure that security is an integral part of information systems

Security Requirements Analysis and Specification

Information Asset Owners and IT shall be responsible for ensuring that specifications of business requirements for new information systems, or enhancements to existing information systems include requirements for security controls, which reflect the business value of the information assets, and are derived from formal risk assessment processes. This equally applies to use of third party software and in-house developed software. Third party software shall be reviewed and evaluated, and third party customer references shall be obtained, to ensure that security requirements are met. Adherence to this information security policy manual shall be a requirement of new and enhanced third party and in-house developed software.

Correct Processing in Applications

Objective: To prevent errors, loss, unauthorised modification or misuse of information in applications

Input Data Validation

Information Asset Owners and IT (as appropriate) shall ensure that all in-house software development includes appropriate validation checks for all input data, and shall ensure that in-house and third party software releases are properly tested for data validation as detailed under System Acceptance above. In addition, Information Asset Owners shall ensure by timely verification that correct data has been entered into operational applications, and shall ensure that any errors are immediately addressed. Users shall immediately report any losses or corruption of data to the Information System Owner or their Line Manager.

Control of Internal Processing

Information Asset Owners and IT (as appropriate) shall ensure that all in-house software development includes validation checks and audit trails to help detect and correct any corruption of data through processing errors or deliberate acts, with appropriate error reporting Office Management Services. Information Asset Owners, IT and users shall also follow policy under Input Data Validation above to ensure that data integrity is maintained within applications.

Message Integrity

Information Asset Owners and IT (as appropriate) shall assess and implement any rrequirements for ensuring authenticity of, and protection of message integrity in applications, based on information risk. Cryptographic techniques shall be considered, and this shall involve use of the policies under Cryptographic Controls below. In addition, consideration shall be given to Vivio's Information Classification requirements above.

Output Data Validation

Information Asset Owners and IT (as appropriate) shall ensure that all in-house software development includes output data validation checks to ensure that the processing of stored information is correct and appropriate to the circumstances e.g. only authorised staff have access to sensitive information. Information Asset Owners, IT and users shall also follow policy under Input Data Validation above, to ensure output data validation.

Cryptographic Controls

Objective: To protect the confidentiality, authenticity or integrity of information by cryptographic means

Policy on the Use of Cryptographic Controls

IT shall be responsible for all cryptography controls (encryption and digital signatures) used by Vivio for the storage and transmission of sensitive information. No cryptography shall be used without the authorisation of IT. Appropriate cryptographic controls shall be applied to protect the confidentiality and integrity of information when justified by risk assessment, and in line with Payment Card Industry Data Security Standard (PCI DSS) requirements and Vivio's Information Classification requirements above.

Key Management

When cryptography is implemented by Vivio, cryptographic keys shall be securely managed throughout their lifecycle, from generation and distribution through to their usage, revocation, archiving and destruction. IT shall be responsible for ensuring that appropriate procedures and controls are implemented and documented, and that they are in line with PCI DSS requirements.

Security of System Files

Objective: To ensure the security of system files

Software shall only become operational when the policies defined under Change Management and System Acceptance above have been applied. Only IT shall install or update operational software and applications, using configuration management processes. IT shall ensure that all computer systems, e.g. servers, PCs and laptops are 'locked down' so that no unauthorised software can be installed.

Protection of System Test Data

By default, live data shall not be copied and used for testing purposes without scrambling or removing any sensitive details e.g. personal information, including credit card details. When it is impractical to do this, measures shall be taken to protect test data from unauthorised access, using physical and logical security controls that provide the same levels of protection as for live data. All copies of sensitive live data shall be formally authorised by Information Asset Owners and IT. Vivio's Information Classification requirements (above) shall be taken into consideration when using sensitive live data as test data. All copies of sensitive live data shall be erased as soon as possible following testing. Information Systems Owners, IT and users involved in testing shall be responsible for the protection of system test data.

Access Control to Program Source Code

In-house developed software shall be protected with access restrictions and version control, in order to maintain the integrity of applications and their security controls. Previously implemented software versions (along with the associated data and procedures) shall be securely archived in case access and use is required at a later date. IT shall ensure that procedures are in place for secure access control and version control of program source code. These procedures shall include proper testing and acceptance of code before it is 'checked' into the software library.

Security in Development and Support Processes

Objective: To maintain the security of application system software and information

Change Control Procedures

Policy on change control procedures for applications' software changes is detailed under Change Management above. This also includes changes to any database information made outside of an application e.g. by use of SQL.

Technical Review of Applications after Operating System Changes

When operating systems are changed, in-house developed applications (if relevant) shall be reviewed and tested to ensure there is no adverse impact on the applications' operation and security. This shall be done by implementing the Change Management and System Acceptance policies above.

Restrictions on Changes to Software Packages

Modifications to third party software packages shall be discouraged, limited to necessary

changes, and all changes shall be strictly controlled. No modifications shall be permitted without authorisation from the Information System Owner and IT. If modifications are necessary, consideration shall be given to the risk of built-in controls and integrity processes being compromised, whether the consent of the vendor is required, the possibility of obtaining the required changes within the next vendor software release, and the impact if Vivio becomes responsible for future maintenance of the software as a result of the changes. All modifications shall be done by implementing the Change Management and System Acceptance policies above.

Information Leakage

Opportunities for information leakage from applications software shall be prevented. Third party ssoftware shall be obtained only from reputable and trusted sources. In-house developed software shall be developed and tested using the policies outlined in this section (Information Systems Acquisition, Development and Maintenance), which shall include use of best security practices e.g. use of the Open Web Application Security Project (OWASP) guidelines for the development of secure web applications. In addition, IT shall monitor systems activity and resource usage for unusual activity, as detailed under Capacity Management above.

Outsourced Software Development

When relevant, any outsourced software development shall be supervised and monitored by Vivio. All contractors shall be required to adhere to this information security policy manual. Policy outlined in Addressing Security in Third Party Agreements above shall be implemented. In addition, all software shall be tested and controlled by implementing the Change Management and System Acceptance policies above.

Technical Vulnerability Management

Objective: To reduce risks resulting from exploitation of published technical vulnerabilities

Control of Technical Vulnerabilities

IT shall be responsible for protecting Vivio from technical vulnerabilities by acquiring timely information about the vulnerabilities, evaluating Vivio's exposure to the vulnerabilities, and implementing appropriate measures. IT shall determine suitable information sources that regularly identify technical vulnerabilities e.g. hardware and software vendors. Procedures and resources shall be established to ensure that information sources are regularly checked for new vulnerabilities. Any actions required to address potential vulnerabilities e.g. the application of security patches shall be carried out in accordance with the Change Management and System Acceptance policies above, as well as Payment Card Industry Data Security Standard (PCI DSS) requirements.

Systems at high risk shall be identified and addressed immediately. Where a vulnerability has been identified, but no security patch is available, other controls shall be considered including turning off services or capabilities associated with the vulnerability, adapting or adding access controls, increasing access monitoring, and raising staff awareness of the vulnerability. The technical vulnerability management process shall be regularly reviewed to ensure its effectiveness.

Information Security Incident Management

Reporting Information Security Events and Weaknesses

Objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken

Reporting Information Security Events

'Security events' are events that could lead to actual security incidents occurring such as unauthorised access to Vivio's (and its customers') information. Examples of security events include a security door being left open whilst unattended, or a user disclosing their password to another user. The Information Security Officer shall ensure that documented procedures and forms exist for reporting and recording all information security events and incidents. Users shall immediately report security events and incidents (actual or suspicious) to appropriate Vivio personnel by following Vivio's Information Security Incident Reporting procedure.

Reporting Security Weaknesses

Responsibilities and procedures identified under Reporting Information Security Events (above) shall also be used for reporting security weaknesses. Users shall not attempt to remedy any detected security weaknesses; otherwise they shall be liable for their actions and may be subject to disciplinary procedures and even legal action. Users shall not continue to use information processing Office Management Services once a weakness has been discovered without reporting the weakness and without acquiring authorisation to continue from their Line Manager and IT.

Management of Information Security Incidents and Improvements

Objective: To ensure a consistent and effective approach is applied to the management of information security incidents

Responsibilities and Procedures

Examples of information security incidents include information system failures, incomplete and inaccurate data, virus attacks, unauthorised access to an information system, computer misuse, fire and theft. The Information Security Officer shall ensure that documented procedures and forms exist for managing all information security incidents. The procedures shall ensure that Vivio is able to respond as soon as possible to security incident occurrences, identify security incident causes, resume a 'business as normal' status as quickly as possible, produce suitable remedies to prevent reoccurrences of security incidents, and gather and securely handle required evidence needed for production in a court of law or for disciplinary cases.

The procedures shall ensure that relevant staff are involved as quickly as possible, and that effective communication surrounding incident management exists within Vivio. IT, Human Resources, Office Management Services, Information Asset Owners and Finance Department (regarding legal requirements) shall ensure that procedures within their own areas of responsibility are documented and implemented.

Learning from Information Security Incidents

The Information Security Forum and Information Security Officer shall ensure that procedures are established to regularly review security incident occurrences in order to introduce improvements and prevent further occurrences. There shall be mechanisms in

place to enable the types, volumes, and costs of information security incidents to be quantified and monitored. A summary of security incident occurrences and impacts shall be included in regular reports to Vivio's Senior Management Board.

Collection of Evidence

Procedures referenced under Responsibilities and Procedures above shall include responsibilities and procedures for the secure collection, retention and presentation of evidence for a court of law, should this be necessary. Vivio shall ensure that the evidence conforms to the rules for evidence laid down in the relevant jurisdiction(s). The procedures shall involve Vivio's Finance Department (for legal requirements) and the Police as necessary.

Business Continuity Management

Information Security Aspects of Business Continuity Management

Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption

Including Information Security in the Business Continuity Management Process

A managed process shall be developed and maintained for business continuity throughout Vivio that addresses the information security requirements needed for Vivio's business continuity. The Business Continuity Management Team shall ensure that information security is included in the business continuity management process.

Business Continuity and Risk Assessment

Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security. The Business Continuity Management Team shall ensure that this process is properly managed. Information Asset Owners and IT shall have a complete understanding of business impacts resulting from losses or unavailability of Vivio's IT network and information systems.

Developing and Implementing Continuity Plans Including Information Security

Vivio shall ensure that it has defined and implemented a Vivio-wide business continuity management strategy and plan, based upon the outputs of on- going risk assessments, and which take into account the relative importance of each information system belonging to, or provided by Vivio. Plans shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required timescales following interruption to, or failure of, critical business processes.

These requirements shall be managed by Vivio's Business Continuity Management Team, who shall maintain the overall business continuity plan. Information Asset Owners shall document their own business continuity plans. They shall have a

complete understanding of their dependencies on IT, sites and buildings, staff and third parties, and the costs involved. IT shall ensure that disaster recovery plans are in place to support business continuity management requirements for IT. Disaster recovery plans shall include any necessary off-site arrangements with third party service providers for critical systems. The business continuity and disaster recovery plans and copies of Vivio's information and software shall be securely stored and managed at two separate physical locations (at least), which are at a suitable distance apart to counteract disasters such as an aeroplane crash.

Business Continuity Planning Framework

The Business Continuity Management Team shall ensure that a single framework of business continuity plans is maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.

Testing, Maintaining and Re-assessing Business Continuity Plans

Procedures shall be in place to regularly test, review and update business continuity and disaster recovery plans, to ensure that they are up-to-date and effective. The Business Continuity Management Team shall be responsible for ensuring that the overall business continuity plan is regularly tested, reviewed and maintained. Information Asset Owners and IT shall support this process by regularly testing, reviewing and maintaining their own plans. Regular testing of business continuity and disaster recovery plans shall be undertaken according to a planned timetable which has been approved by Vivio's Senior Management Board.

Compliance

Compliance with Legal Requirements

Objective: To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements

Identification of Applicable Legislation

Vivio shall regularly review new and changing legislation that affects its information security policy, and shall immediately implement relevant changes. Finance Department shall be responsible for providing advice and guidance to ensure that Vivio complies with its legal, statutory, regulatory and contractual obligations. The Information Security Forum shall regularly review legal obligations that influence this policy, and the Information Security Officer shall update policy as and when necessary. Information Systems Owners and IT shall maintain records of all legal, statutory, regulatory and contractual requirements relating to the IT network and information systems under their responsibility.

Intellectual Property Rights (IPR)

All users shall comply with intellectual property rights and copyright legislation and contracts, including the Copyright, Design and Patents Act, 1988. Software used with Vivio's information processing systems shall only be used in line with Vivio's Authorisation Process for Information Processing Office Management Services above. Users shall follow policy provided in Vivio's Information Security User Guide, and shall comply with Vivio's E-mail, Phone and Internet Usage Policy. IT shall manage software assets and licenses in line with policy under Inventory of Assets above.

IT shall use formal procedures to manage and protect software and licenses. Only licensed copies of commercial software shall be used and a register of licences shall be held by IT, with evidence of ownership. Software and licenses shall be regularly audited for legal compliance. Users shall not copy and distribute software and hardcopy documentation that is copyright protected without authorisation from their Line Managers and IT.

Protection of Organisational Records

Vivio shall implement and maintain records of its information assets within a Records Retention and Disposal Policy and Schedule, to protect information from loss, destruction and falsification. This document shall identify all valuable information assets that belong to Vivio, and shall be maintained by Vivio's Senior Management Board. Information Asset Owners shall regularly notify Vivio's Senior Management Board of any required changes to the Records Schedule. The policy and schedule shall address all legal, regulatory, contractual and business requirements of Vivio for the retention and disposal of information. They shall indicate information retention timescales, suitable methods of information storage, and information disposal requirements. This includes requirements for application data, documents, files, and audit trails, and valuable information that is stored in electronic, media and hardcopy formats. Vivio's Information Classification requirements (above) shall be taken into consideration.

Data Protection and Privacy of Personal Information

Finance Department shall be responsible for implementing Vivio's legal requirements for data protection. This includes notifying the Information Commissioner about Vivio's use of personal data, and documenting data protection policy, procedures and guidelines. Vivio shall also appoint suitable data protection representatives within each of its directorates and business units to facilitate implementation of data protection requirements. Information Asset Owners or their data protection representatives shall immediately notify Finance Department of any changes in their processes that involve personal information and that have legal consequences. All users shall comply with Vivio's Data Protection policy, procedures and guidelines e.g. dealing with data subject access requests. Finance Department shall ensure that staff receive appropriate training and are aware of the requirements of the Data Protection Act.

Prevention of Misuse of Information Processing Office Management Services

Users shall comply with this information security policy manual, and its supporting sub-policies, procedures and guidelines e.g. Vivio's E-mail, Phone and Internet Usage Policy, and shall comply with the Computer Misuse Act, 1990. Users shall not attempt to use computer systems to gain unauthorised access to information and software, or to cause system outages. Users shall not deliberately introduce malicious software such as computer viruses onto Vivio's network infrastructure and information processing systems.

Regulation of Cryptographic Controls

IT shall ensure that cryptographic controls are used in compliance with all relevant agreements, laws, and regulations. Policy on the Use of Cryptographic Controls (above) shall be implemented.

Compliance with Security Policies and Standards, and Technical Compliance

Objective: To ensure compliance of systems with Vivio's security policies and standards

Compliance with Security Policies and Standards

Information Asset Owners and Line Managers shall ensure that all security procedures within their areas of responsibility are carried out correctly to achieve compliance with this security policy, and its procedures and controls. All areas within Vivio shall be subject to review by the Information Security Officer to ensure compliance with this policy.

Technical Compliance Checking

Information systems and the IT network shall be regularly checked for compliance with this policy, the Payment Card Industry Data Security Standard (as relevant), and with other security implementation standards, as defined by reputable information security industry sources, and taken on by Vivio to protect its information systems. Vivio's network infrastructure and information processing systems shall be subject to regular independent technical compliance checks e.g. penetration testing, including whenever significant changes are being implemented into the operational environment. These checks shall be carried out by a competent, authorised person(s) or third party organisation with specialist technical expertise. IT shall ensure that technical compliance checking is regularly undertaken.

Information Systems Audit Considerations

Objective: To maximise the effectiveness of and to minimise interference to/from the information systems audit process

Information Systems Audit Controls

Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to minimise the risk of disruptions to business processes. Procedures for the management of information systems audits shall be documented and implemented by the Information Security Forum and the Information Security Manager.

Protection of Information Systems Audit Tools

IT shall implement physical and logical access controls to restrict access to any information systems audit tools used by Vivio, to prevent any possible misuse or compromise. Audit tools shall be held separately from development and operational systems and not held in tape libraries or user areas. Similarly, IT shall ensure that unauthorised users are not capable of executing 'hacking' and auditing software that has been acquired from the Internet or other external sources.