Encana

Information Security Practice

encana

Table of contents

1 Introduction

1.1 Introduction and audience

Intent: This document defines Encana's baseline information security control requirements for protecting corporate information and IT assets. Standard requirements applicable across the corporation ensure that Encana's IT assets and digital information are suitably protected from security breaches that could adversely impact Encana's business, reputation, cause a regulatory breach or impact personal safety or the environment. It defines the mandatory principles and high-level security requirements to control information security risks in accordance with Encana's information management policy .

Primary readership: This document is intended for leads, group leads and team leads etc. who sponsor the procurement, creation or maintenance of IT assets in support of their business processes; and for IT staff and others who are accountable or responsible for Encana digital information or IT assets. Primary readership includes, including those who:

- act as single points of accountability (SPAs) for IT assets as defined below, and their delegates, or
- are involved in procuring, managing, developing or operating Encana's IT assets (e.g. project managers, operating managers, contractors and outsourced service providers;)

Additional requirements: Additional risk-based controls may be specified by the practice owner for IT assets with high criticality. More detailed controls based on these principles and applicable to specific types of IT assets, may be defined by the practice owner to support standards and guidelines.

1.2 Applicability, responsibilities and terminology

The control requirements in this practice apply to all of Encana's electronic information and to all IT systems operated by or for Encana. This includes IT systems, applications, services and infrastructure, both in their development and deployment, and in their day-to-day operation and use.

These controls need not be applied retrospectively to IT assets implemented at the date of approval unless specifically directed by the practice owner. However, the requirements in this document do apply to new assets and to existing assets that are changed.

Encana leaders must enforce compliance by their staff (employees and contractors) with Encana and business unit and corporate groups requirements for the acceptable use of IT systems including Encana's acceptable use practice.

Applicability

This practice applies to Encana as a whole and is mandatory across all divisions and corporate groups. It applies to all IT assets used in relation to Encana's operations, whether wholly owned and operated by Encana or externalized because of outsourcing, external suppliers or joint ventures.

The practice also applies to IT assets used in relation to Encana's activities and operated by third parties contracted to Encana, or operated by joint ventures in which Encana is involved wherever Encana has sufficient control to influence contract terms.

Where it is not feasible to require a joint venture or contractor to adopt this practice or where a joint venture or contractor has already agreed to adopt a previous Encana policy, Encana will seek to influence or persuade the joint venture or contractor to adopt security controls consistent with this practice.

Terminology

Capitalized terms in this document, plus the words "must" and "should" are defined in the glossary for Information Security Practice which is maintained here. Terms of particular importance are below.

"Must" and "should": the words "must", "shall", "will" and "required" mean that the item is a mandatory corporate requirement and that no deviation without an approved waiver or dispensation is permitted.

The words "should" and "recommended" are defined in the glossary and mean that a security control is security practice whose application is strongly recommended, but which is not mandatory in all circumstances.

Single point of accountability (SPA): SPAs are members of Encana Leadership who sponsor the procurement, creation or maintenance of one or more IT assets in furtherance of division or corporate group business processes and services for which they are accountable, or Encana staff with appropriate business knowledge who have explicit delegation from such a member of Encana Leadership.

An IT asset SPA is the single point of accountability for the viability, security and resilience of an IT asset. SPAs ensure all security procedures within their area of responsibility are carried out correctly to achieve compliance with this security practice, and that access to their IT assets is properly authorized, reviewed and limited to what is appropriate for business purposes.

IT assets are defined in the glossary and include Encana digital information; and all digital infrastructure, operating systems, applications, IT-related support services, and externalized digital information processing and storage services used to store or process Encana digital information. IT assets are not limited to infrastructure, systems and services maintained or procured by Encana information services.

The glossary: Capitalized terms in this document are defined in the glossary for information security practice.

1.3 Deviations, waivers, risk acceptance and violations

Deviations and risk acceptance: it is recognized that there may be occasions when a SPA determines that requirements of this information security practice are impractical or carry a cost disproportionate to the risk. A SPA may choose to accept the risk of non-application of standard controls (within limits).

A SPA will be permitted to accept the risk of omission of a mandatory control or its incomplete or delayed implementation when a waiver has been obtained and recorded. A SPA may accept the risk of deviation, potentially without mitigating controls, provided that:

- any regulatory or legal implications or breaches of control standards established by other Encana corporate groups have been covered by alternative mitigating controls and have been agreed to by the relevant corporate group or regulator
- risks and any wider impacts on the corporation have been assessed in accordance with the risk assessment process approved by the practice owner and have been reported in accordance with line management reporting processes

- a date is given by which the risk acceptance will be reviewed
- the risk acceptance and related risk assessment are reported to the practice owner for aggregate recording, potential challenge and escalation to the relevant risk authority who may accept or overturn the decision

Waiver: A waiver is required where, in the opinion of the practice owner risk is likely to result that will not have corporate materiality as long as the delay in implementation or incompleteness of implementation is controlled. Waivers will be granted on a temporary basis and require joint approval from the practice owner and affected stakeholders.

Violations of this practice will be considered a breach of Encana corporate policy and may result in disciplinary actions that may include, among other actions, dismissal or legal action. Reports of violations of this practice will practice will be forwarded to the appropriate business unit or corporate group leader, human resources, information security and the and the investigations committee if relevant. In cases where local or international law is violated, Encana has a responsibility to involve the relevant law enforcement agencies.

1.4 Practice administration and authorization

Practice Owner: Steve Biswanger, Team Lead, Information Security

Interpretation: Questions of interpretation relating to this practice may be directed in writing to the practice owner listed above for clarification.

Document control and review: This document is subject to review on two year intervals or when significant changes occur within the Encana environment. All reviews will be initiated by the practice owner at his or her absolute discretion.

Last document review date: January 2013	**Next document review date:** January 2015

2 Practice statements

2.1 Information security risk management

2.1.1 Assess security risks

1. In order to ensure that information security risks are effectively managed they must be systematically identified, assessed and treated. Encana leaders will ensure that risks pertaining to Encana IT assets (including Encana information) are identified and assessed using the risk methodology provided by the practice owner.

2.1.2 Assess criticality

1. IT asset SPAs and information owners will use the risk methodology provided by the practice owner to assign an appropriate criticality to their IT assets. Criticality ratings shall be based on business impacts and priorities, as determined by relevant Encana team leads and above.

   The criteria include:

   a. whether the system supports key business processes or processes critical to safety or the environment;

   b. the sensitivity and classification of the information stored or processed by the system;

   c. the business impact of a security breach in relation to the asset, including impacts on other IT assets or business processes; and

   d. whether the asset supports business processes that are subject to legal or regulatory controls and the potential repercussions from non-compliance if there is an information security failure

   SPA determination of criticality may be challenged by the practice owner. In the event of a dispute, criticality will be determined by the relevant Vice-President or Executive Vice-President, or their delegate.

2. Where an IT asset has high criticality according to the risk methodology the SPA will:

   a. report this to the practice owner who will assess the security risks associated with the asset; and

   b. in conjunction with the practice owner, determine any security controls in addition to the standard controls in the information security practice to be applied and the timing for compliance

2.1.3 Standard controls as a minimum

1. SPAs and staff who procure, implement, develop, change or operate IT assets must:

   a. ensure that all IT assets are, at a minimum and regardless of criticality, compliant with the controls in this practice that are applicable to them; and

b. apply any additional security controls or requirements identified in accordance with the risk methodology provided by the practice owner

2.2 Access control and management

2.2.1 Access authorisation

1. Physical and logical access to IT systems and digital information as well as alterations to access must be authorized before access or change to access occurs. SPAs must nominate an individual with suitable knowledge of potential business impact who is delegated with this authority and becomes an access authorizer.

2. the identity of access authorizers as well as the details of their authority (position) must be recorded

3. access authorizers must specify and record the level of access to be granted to each account

4. staff must not be authorized to access any Encana IT system or information until they have signed acceptance of Encana's acceptable use practice

2.2.2 Account types

1. all accounts must follow a standard naming convention that identifies the type of account and whether it is:

   a. used by individuals or groups;

   b. used only for privileged (e.g. administrative) activities by individuals;

   c. used only for system-to-system processes by IT Systems;

   d. a temporary test account;

   e. used only for vendors' remote support; or

   f. used only for access that does not require network logon privileges

2. Accounts must be used only for their designated and authorized purpose, e.g. standard accounts are used only for normal-user network logon and non-privileged activities. System-to-system accounts on production systems must not be used by individuals by interactive logon; and. Privileged accounts must not be used for normal user activities or to circumvent security or access controls.

3. Exceptionally, system-to-system accounts may be used interactively for temporary testing. This use must be logged and must be approved in writing by authorizing SPA.

4. Encana account types are standard, elevated, generic, service, vendor and test, as defined in the glossary and must comply with Encana password standards

2.2.3 Access control

1. access authorization should be based on business need and provide the least access level that is reasonably necessary to allow completion of the required duties or services

2. for critical Encana IT systems and information classified confidential or restricted, or that requires protection by law, by policy or by agreement, access authorization must be based on business need and only provide the least necessary access level to allow completion of the required duties or services

3. accounts which perform privileged or administrative functions, or which provide access to back-end services or processes (elevated, vendors and service accounts) must be configured with "least privilege", i.e., the minimum set of access rights needed to carry out the account's business purpose

2.2.4 Accountability

1. All IT systems managed or operated by or for Encana must be auditable. An auditable system is one where each transaction is capable of being logged and linked to the access account that performed it.

2. there must be a specific account owner associated with each access account to establish individual accountability

3. each individual assigned a single-user access account (standard, elevated and vendor accounts) is the considered the account owner of that account and is accountable for all actions undertaken using it

4. activities under standard user accounts on IT systems operated by or for Encana must be uniquely linkable to the individual performing the activity so that he or she can be held responsible for his or her actions

5. individual activities under access accounts with elevated privileges on IT systems operated by or for Encana (elevated and vendor accounts) must be uniquely linked to the individual performing the activity for all administrative and support activities, including database and operating system support activities

6. the account owners of service accounts and generic accounts are recorded and are accountable for all actions undertaken using those accounts

7. generic accounts are permissible only when access is limited to actions that do not require individual accountability or when individual accountability is retained by other means

2.2.5 Segregation of duties

1. provisions for segregation of duties should be considered for all business and IT processes, systems, networks and applications and should be designed in such a way to prevent a single individual (whether user or system administrator) from making unauthorized changes or committing fraud by:

   a. creating a transaction and then approving the transaction;

   b. requesting access to a resource and then approving this access; or

   c. authorizing access and then processing the access request

2. for critical IT assets, and for information or processes that are particularly valuable or sensitive, or where the actions of a single individual may have material Impact (e.g., environment, health, safety, reputation or financial risk), segregation of duties is strongly recommended as a safeguard to prevent or limit to a defined degree the ability of any single individual (whether user or system administrator) to make unauthorized changes or to commit fraud

2.2.6 Account provisioning and review

1. account creation/change/deletion may only be performed by authorized persons, and only when authorized to do so

2. password change or reset may only be authorized by the account owner or, in his absence, by information security.

3. IT asset SPAs must ensure regular review of all access accounts for their IT assets. The review should include confirmation that access and privileges granted are still necessary for the individual or account's role, confirmation that processes for account review on role changes or termination of employment or contract remain effective and for service, group and vendors' accounts, confirmation of the account owner.

2.2.7 Authentication and credentials

1. Authentication credentials for single-user accounts must be known to only the individual to whom the account is issued. Authentication credentials for service accounts and generic accounts must be known or held only by the specific individuals authorized by the IT system SPA or his access authorizer.

2. credentials must be unique to the account, i.e., the same credential or password must not be used for multiple accounts

3. except where password change would create unacceptable health, safety, environmental or financial risk, passwords for access accounts to IT systems are changed promptly after disclosure to

any unauthorized individual and when a previously-authorized person no longer requires access, e.g., when someone leaves the group in the case of generic accounts, or someone leaves the support team in the case of service accounts

4. in all situations other than anonymous access to public information (e.g. www.encana.com), access to IT systems and digital information (including operating systems, applications and databases) must be authenticated

5. Authentication credentials must provide appropriately secure verification of the identity of the account user or process commensurate with the account's privileges, the classification of information or systems to which it has access and the trustworthiness of the originating operating system and location. For generic accounts, "verification of the identity of the account user" means verification as a member of the authorized group.

6. access account credential complexity, expiry, lockout and maximum age must be sufficient to provide reasonable certainty of identity, and protection from disclosure by automated or other "guessing"

7. Authentication mechanisms employed by IT systems must maintain the security of credentials. Specifically, authentication credentials for access to IT systems including applications and databases must not be transmitted in a form that can be decrypted or replayed if intercepted, and, if stored in any manner, must be stored in a form that is secure (preferably by non-reversible encryption).

8. credentials must not be embedded within application code or scripts unless authorized by information security

9. Passwords must not be transmitted outside of networks managed by or for Encana in clear text or in any form that can be decrypted or replayed if intercepted. This includes individuals' passwords and passwords used for authentication between systems and/or processes.

10. passwords that are communicated over networks managed by or for Encana are encrypted when possible and should be protected from capture and replay

11. account owners have sole responsibility to ensure that assigned passwords are kept confidential

12. Passwords for generic and service accounts maybe shared with individuals who have a business need to know. Identities of individuals to whom passwords are communicated must be recorded and passwords must be changed when an individual leaves that group. Passwords for individual accounts (standard, elevated and vendors) must not be shared with any other individual.

13. access controls for an application, database or other data storage device must not be compromised by weaker access controls on the infrastructure on which it operates

2.3 Internetworking

2.3.1 Network connections

1. communications and data that traverses the boundaries of Encana networks, the boundaries of private networks shared with other parties or the boundaries of specialized Encana networks (e.g., data centers, wireless, development networks, process control networks) must be authorized, monitored and controlled by security gateways (firewalls, gateways or routers with monitored traffic filtration) which are managed, monitored and controlled by or for Encana

2. Only authorized IT systems (e.g., PCs, laptops, tablets, printers, wireless access points) may be connected directly to any network managed by or for Encana. In the case of Encana's guest networks (Extended Internet Access (EIA) and Wireless Internet Access (WIA)), "authorized" means that the device's user has agreed to Encana's internet guest access agreement.

2.3.2 Security gateways

1. security gateways must be capable of and configured to allow only communications that are explicitly approved to support a defined business need

2. security gateways should include layered security defense systems such as firewalls, anti-virus systems, intrusion-detection systems, content filters and spam shields

2.3.3 Remote access

1. inbound connections across external boundaries of Encana networks, including access to Encana networks or to Encana IT systems from private networks shared with other parties must be authorized and, other than anonymous access to Encana public information (e.g. www.encana.com), must be authenticated

2. remote access to Encana digital information by external parties who do not possess Encana access accounts, whether for collaboration, file transfer or exchange, must be authorized by the relevant IT system SPA and information owner and must be authenticated by credentials consistent with this practice

3. remote access to Encana digital information or IT systems should, when possible, be limited according to the trustworthiness of the originating operating system and location

4. users of Encana's remote access services should ensure their personal remote access connection and computing system is secure

5. Remote access for maintenance occurs only when authorized. Sessions or connections are terminated when maintenance is complete. If that is not possible they are monitored for unauthorized use.

2.3.4 Mobile devices

1. mobile electronic devices which connect to Encana IT systems, or connect to or store Encana information must be protected by access controls commensurate with information classification and the device must be secure

2.3.5 Off-premises devices

1. IT devices used outside secured Encana premises must themselves be protected with appropriate physical and logical access controls according to the sensitivity and business value of the information being processed or displayed, and with controls equivalent to those required for IT devices within Encana premises

2.4 IT asset acquisition and development

2.4.1 Identify security requirements

1. in all projects involving the procurement, deployment, development or change of IT assets, information security risk must be assessed as an integral part of project risk assessments

2. Encana leaders and IT asset SPAs accountable for procuring, implementing, developing or changing IT assets, including applications, systems, services or infrastructure, must implement security controls appropriate for secure deployment, operation and use of the IT asset being procured or developed, including security controls for the development process itself as set below or as directed by Encana information security

3. IT asset procurement and development will include appropriate pre-deployment security testing and fallback arrangements

4. development controls will include segregation of programmer access from the production environment and segregation of coding and migration permissions

2.4.2 Application security

1. Critical IT systems must include security controls to ensure secure processing. Secure processing controls may include session management, the validation of input and output data, verification of message integrity and internal processing, validation of output data, error reporting and secure output handling.

2. web applications should include security controls to address the relevant issues in the open web application security project (OWASP) top web application security flaws and the published SANS/MITRE top 25 software errors and SANS/MITRE top 25 software errors

3. if network communication of confidential or restricted information traverses networks that are not fully trusted or not fully under Encana control (e.g., the internet), data sent or received must be protected against eavesdropping in transit using strong encryption

4. user sessions in IT systems processing financial information or information that is confidential or restricted must use session IDs that are cryptographically secure or otherwise protected against session hijacking or information reuse if that is technically possible

5. critical IT systems, and IT systems accessing, storing or processing information that is confidential or restricted must suspend user sessions after a period of inactivity unless session or system lockout creates unacceptable risks e.g. health and safety, in which case they should be physically secured when unattended

6. Applications involving significant financial transactions must include controls to protect against fraudulent activity. Such controls may include segregation of duties, or dual controls over set transaction limits, which prevent or limit to a defined degree the ability of any single individual (whether user or system administrator) to commit fraud, and relevant controls specified by finance.

7. projects developing custom designed software should be supervised and monitored and should use a secure software development lifecycle materially consistent with the systems security engineering capability maturity model (ISO/IEC 21827:2008) or Microsoft's trustworthy computing security development lifecycle

8. systems which process significant financial transactions, or which store, process or transmit confidential or restricted information must use a secure software development lifecycle

2.4.3 Standard infrastructure security configurations

1. if multiple instances of an IT system will be deployed, the SPA must ensure that a documented standard configuration is developed, which implements baseline IT security controls and security settings to be applied to all instances of the system's architecture

2.4.4 Contractual development controls

1. IT system procurement or development contracts must specify security controls and procedures for IT system and software development that meet or exceed the controls specified in this practice

2.4.5 Data sanitization in development and testing

1. Personal information, confidential and restricted information must not be used for application development or testing purposes without the approval of the SPA, practice owner and the information owner, who must ensure that any such use conforms to legal and regulatory requirements. It is strongly recommended that anonymised data be used for testing purposes.

2. access controls in development environments, including encryption at rest, logging and access review, should be equivalent to production environments

3. for critical systems and systems which access, store or process confidential or restricted information, access controls in development environments, including encryption at rest, logging and access review, must be equivalent to production environments (which require log and review of privileged-level access)

2.4.6 Secure by default

1. applications and infrastructure must be designed so that configurable security settings are enabled when installed, i.e., "secure by default"

2.4.7 Security testing

1. Pre-implementation test plans should (for critical IT systems and internet-facing systems, "must") be established to verify the implementation of all applicable requirements in this document. Testing techniques may include any or all of code reviews, segregation of test environments, penetration testing, resilience testing and security functionality testing. Test plans should be designed to support interim testing when significant changes occur.

2. penetration testing and vulnerability assessment tools must not be used without the prior written approval of information security

3. IT systems must not be released for use in a production environment until identified security issues have been resolved unless a signed waiver is obtained with written acceptance of residual risks at the appropriate level of accountability

2.4.8 Segregation of development and production

1. test and development environments should be logically separated from production environments

2. test and development environments for infrastructure including middleware, and for applications which process significant financial transactions, or which store, process or transmit confidential or restricted information must be logically separated from production environments if that is technically possible

2.5 Security incident reporting and response

2.5.1 Security event reporting

1. all observed IT security events and incidents (observed system, network or user behaviour that is suggestive of unauthorized alteration, disclosure or use of or access to Encana systems or Encana Information) must be reported immediately to the Encana service desk

2.5.2 Response to IT security events and incidents

1. IT system SPAs must implement, test and review IT security event and Incident reporting and response plans and processes which ensure the identification, classification, response and reporting of IT security events which have the potential of serious or critical impact

2.6 Operations management

2.6.1 External hosting

1. Any external hosting facility which hosts Encana IT systems or information (including application service providers (ASP), software as a service (SaaS) and "cloud" service providers) must undergo an IT security review to ensure that it meets Encana baseline security control requirements, or must provide evidence that it meets materially equivalent alternate security controls. Compliance with Encana baseline security requirements must be confirmed at least once every two years.

2. IT system SPAs accountable for outsourced IT system hosting, management or support or for outsourced hosting of Encana information must assess security risks and ensure that mitigating controls that are consistent with this practice are implemented and maintained, including:

   a. the IT system SPA ensures that IT security controls that are materially equivalent to this practice are applied to hosting, operation, management and support of IT systems.

   b. the IT system SPA ensures that there are processes in place to ensure that when significant changes are made to outsourced IT systems, all relevant mandatory IT security controls are in place

   c. the IT system SPA ensures that when outsourcing contracts are renewed or changed, risks are reassessed and suitable changes in IT system security controls are included

2.6.2 Operational security procedures and documentation

1. IT asset SPAs must establish and maintain up-to-date and documented operational security processes consistent with relevant requirements in this document for:

   a. change and release management,

   b. IT equipment physical security,

   c. protection against malicious and mobile code,

   d. back-up,

   e. security-related monitoring and logging,

   f. user access management including access provisioning and de-provisioning,

   g. competence of support staff including awareness of and training in security risks and responsibilities, and when relevant to their IT assets; and

h. telecommunications and network management and control

2. IT asset SPAs must ensure that documentation required by this practice is reviewed at least every two years, and when major changes to the asset are implemented

2.6.3 Change management

1. IT asset SPAs must ensure that changes to IT assets are subject to formal change management procedures which include communication of the and confirmation that the mandatory control requirements in this practice are met

   Mandatory control requirements for change management include:

   a. provision for emergency changes

   b. changes to IT assets, whether scheduled or emergency changes, are made according to relevant published change and release processes

   c. changes and additions to IT assets are authorized prior to implementation by the IT asset SPA and also by an individual designated by the relevant business unit(s) as being authorized to approve changes and releases

   d. the change management process ensures that changes to the IT asset are not approved by the person requesting the change

   e. change control documentation is retained, including the date and time of change, the reason for change, the name of the person making the change and the person or persons who authorized the change

   f. the change management process specifies the time scales for non-emergency requests for change or release to ensure that there is sufficient time for review, and for the determination and review of potential impacts

   g. change requests should document at least the reason for change, the impact analysis and any anticipated security risks, including risks to infrastructure or the assets of other IT asset SPAs

   h. change requests are communicated to the SPAs of any IT assets or information that may be adversely affected by the change

   i. if a change or addition to an IT asset fails to meet any mandatory security requirements, and the security non-compliance has not previously been authorized, the change is reviewed and approved by Encana IT security

   j. all non-emergency requests for change or release include contingency provisions, such as roll-back procedures to allow abort and recovery

   k. release of systems from development to production includes handover documentation

2.6.4 Physical security of IT systems

1. SPAs for IT facilities and IT systems (including i.e., data centers, telecommunications rooms, server rooms, UPS rooms, and their backup media) must ensure that physical access is controlled, with access only granted to individuals with legitimate business responsibilities in the facility

2. IT system SPAs for network infrastructure (including i.e., switches, routers, LAN servers, network busses, cabling and wiring) must ensure that access is controlled when technically possible, with physical access only granted to individuals with legitimate business responsibilities in the facility, maintaining physical separation between Encana and non-Encana networking equipment and wiring

3. IT system SPAs for IT facilities and IT systems must ensure that design and operation includes protection from physical and environmental risks such as fire, flood and earthquake, and from risk of interruption in utilities such as power, water and cooling

4. physical protection of IT systems includes protection of media and back-up media, including precautions for secure disposal or re-use and precautions against unauthorized access during maintenance

2.6.5 Competence of support staff

1. SPAs must ensure that security-related skill; training and supervision requirements for support staff (including Encana employees, contractors and outsourced suppliers) are clearly identified and fulfilled as part of the hiring process

2. in addition, SPAs must ensure qualifications of support staff with logical or unescorted physical access to critical IT systems are checked and verified prior to authorization of access

2.6.6 Auditing, monitoring, logging and vulnerability assessment

1. monitoring, logging or “sniffing” of network traffic is prohibited unless authorized by information security or technical security

2. System event logging must be enabled in IT systems for security-related events that have the potential of serious or critical impact. Minimum system logging, if application or operating system allows, includes system/application start/stop times, unsuccessful logon attempts, addition or modification of user credentials and access permissions.

3. IT system SPAs, in consultation with information security, will implement additional logging of system and user activity when necessary in light of system and information criticality and in accordance with legal requirements

4. network traffic monitoring, i.e., passive scanning of network activity, or intrusion detection or prevention), which is continuously monitored is enabled for network traffic at all security gateways

5. when logging is required, IT system SPAs must establish procedures for reviewing the results of monitoring and logging, and for the secure retention of logs

6. access to monitoring logs and information recorded must be limited and controlled in accordance with business need and legal requirements, including privacy and data protection requirements

7. Network vulnerability assessments ("vulnerability scanning") of critical IT systems and networks must be performed regularly to ensure that systems are configured and patched in accordance with Encana standards. Assessments should include at least:

   a. verification that only authorized ports and services are enabled;

   b. review of default accounts and passwords to verify disabling or change, when required; and

   c. verification that required configurations and patch levels are in place

2.6.7 Patching

1. IT system SPAs (either separately or as a component of the change management process,) must establish, document and implement a security patch management program for tracking, evaluating, testing and installing applicable security software patches for all IT systems so as to prevent material risk

2. The security patch management process should include processes to respond to patching requirements specified by Encana technical security within the time scales specified. Alternatively, it should include processes to receive and assess vulnerability and patch availability information for their systems and to receive, assess and implement security-related patches for their systems on time scales that prevent material risk.

3. when patching is impractical because of vendor requirements or application compatibility, IT system SPAs must establish processes to asses risk and implement alternate mitigating controls that will prevent material risk

2.6.8 Anti-virus

1. IT systems that are susceptible to infection or attack by malicious or mobile code, or which can be used as transmitters or receivers of such (i.e., file servers, data historians, databases, PCs, email servers and email clients) must be protected by effective anti-malware software

2. to lessen the threat of network-propagated vulnerabilities, unnecessary network services and ports are disabled or removed

2.6.9 Back-up

1. IT system SPAs of storage systems (e.g., SharePoint and LiveLink data servers, file servers, and database infrastructure) must ensure that storage systems are backed up and restorable in accordance with a documented back-up strategy which is aligned with Encana's records management practice

2. IT system SPAs must create and annually review a backup strategy for their IT systems and business-significant Encana Information to ensure that data recovery and infrastructure recovery is possible in accordance with their documented requirements

3. The usability of back-ups must be verified at least annually. Usability does not need to be verified by each IT system SPA if it has been verified by shared or central verification processes.

4. access to backed-up data must be controlled in a manner at least as strong as the control of access to the data on the system being backed-up

2.7 External parties and outsourcing

2.7.1 Contractual requirements

1. information that is confidential or restricted, or whose unauthorized disclosure, alteration or destruction could cause material impact may not be exchanged with external parties except within the context of a formal contract that includes, at the least, a non-disclosure agreement

2. before access to Encana IT systems is provisioned to external partners, and before they are permitted to process, store or manage Encana Information, terms and conditions for service and access must be established

3. for standard account access by external parties to Encana IT systems or Encana information stored on Encana's corporate networks, IT system SPAs will ensure that a contract is in place that provides for confidentiality and non-disclosure of Encana information, and that ensures compliance with relevant Encana policies and practices including:

    a. information management policy

    b. IT system acceptable use practice

    c. information security classification practice

    d. business conduct and ethics practice

4. Before authorizing the development, control, operation or maintenance of Encana IT assets, or the provision of IT services by external parties, the IT system SPAs must ensure that a formal contract is in place that includes provisions for the security of Encana information and IT systems, and that relevant Encana policies, standards, practices and responsibilities have been communicated to the external party. This includes contracts for:

    a. outsourced application development;

    b. control, operation or maintenance of Encana IT Systems by external parties; or

    c. storage, processing or management of Encana Information on non-Encana IT systems by external parties

5. contracts with external parties for the development, control, operation or maintenance of Encana IT assets, or the provision if IT services should include the standard IT security provisions approved by Encana legal including provision for compliance with Encana's IT security practice

6. external party IT contracts should additionally specify security service level requirements to be implemented by the service provider, such as security incident response times, security notifications to Encana, security patching and security management

7. in the absence of standard security language or in the event of non-use of Encana's standard language, contracts with external parties for the development, control, operation or maintenance of Encana IT assets, or the provision if IT services must contain provisions:

   a. requiring the external party to protect Encana IT systems and information from loss, unauthorized disclosure and alteration in a skilled fashion that is at least as rigorous as the measures used to protect its own most sensitive information and systems;

   b. requiring the external party to fully comply with Encana's information security practice or a well-defined and recognized public standard (e.g. ISO 27002:2005, CSA cloud controls matrix);

   c. providing for the confidentiality of Encana information, including personal information;

   d. allowing Encana to verify that security process and facilities relating to the external party's product or service, including IT Infrastructure provided to the external party by others, comply with security requirements;

   e. requiring the external party to monitor carefully for and to provide prompt notice of security Incidents relating to Encana's information or the products or services provided and to cooperate with Encana in any steps required for remediation; and

   f. ensuring that Encana information and any information derived from that is returned to Encana on conclusion of the contract and on bankruptcy or cessation of business of the supplier if the contract puts the supplier in possession of Encana information or information developed for Encana and when non-availability of the external party's software would have material impact

8. Where a contractual relationship with an external party exists, there must be an Encana employee designated as accountable for IT security in relation to the contract. In addition the external party must specify its own contact to Encana for IT security matters.

2.7.2 Monitoring and review

1. IT system SPAs accountable for IT systems provided by external parties must ensure the periodic review of security controls relevant to the IT systems. This should be consistent with legal requirements and the criticality of the service.

2. periodic reviews of external party contracts for IT systems must confirm the implementation of contractually specified security control requirements and/or security service levels

2.8 Disaster recovery planning

1. Recovery plans must be put in place for IT systems where disruption would cause material impact, whether directly or because of consequent disruption of dependant IT systems. Recovery plans should follow established business continuity and disaster recovery techniques and practices including testing and re-evaluation.

2. IT system SPAs must establish disaster recovery and/or service resiliency, availability, continuity plans consistent with business unit and regulatory business continuity requirements, if any

3. Recovery plans should be tested at least annually. Testing may range from a paper drill to a full operational exercise.

4. recovery plans should be re-evaluated and updated following annual testing and major business change