IT Security Policy

CALEDONIAN SCHOOL OF ENGLISH

Developed with the assistance of

FORTRUST

and

SANS Institute

Updated 21/05/2020

1 IT SECURITY POLICY

Purpose

The purpose of this policy is to protect from all threats, whether internal or external, deliberate or accidental, the information assets of:

CALEDONIAN ENGLISH;

Students/Clients;

Staff/Teachers;

Partners/Affiliates;

1.1 OBJECTIVES

The implementation of this policy is important to maintain and demonstrate our integrity in our dealing with customers and suppliers.

It is the policy of **CALEDONIAN ENGLISH** to ensure:

- Information is protected against unauthorised access
- Confidentiality of information is maintained
- Information is not disclosed to unauthorized persons through deliberate or careless action
- Integrity of information through protection from unauthorised modification
- Availability of information to authorized users when needed
- Regulatory and legislative requirements will be met

- Business continuity plans are produced, maintained and tested as far as practicable
- Information security training is given to all Employees
- All breaches of information security and suspected weaknesses are reported and investigated

1.2 APPLICABILITY

All **CALEDONIAN ENGLISH** personnel and suppliers, employed under contract, who have any involvement with information assets covered by the scope of the Information Security Management System, are responsible for implementing this policy and shall have the support of the **CALEDONIAN ENGLISH** Management who have approved the policy.

1.3 GOALS

- To identify through appropriate risk assessment, the value of information assets, to understand their vulnerabilities and the threats that may expose them to risk.
- To manage the risks to an acceptable level though the design, implementation and maintenance of a formal Information Security Management System.
- To comply with EU Data Protection Standard GDPR: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations_en.
- To comply with any customer contract conditions relating to information security.
- Commitment to comply with ISO 27001-2005
- Commitment to achieve and maintain certification to ISO27001-2005

Specific Policies

Specific policies exist to support this document including:

- ACCEPTABLE USE POLICY (email, internet access, access control, software download)
- CLEAN DESK POLICY
- ROUTER AND SWITCH SECURITY POLICY
- PASSWORD PROTECTION POLICY
- DATA BREACH RESPONSE POLICY

Other Policies

Other internal documents and policies exist to support this document including:

- CALEDONIAN ENGLISH (CE) COMPANY HANDBOOK
- PHYSICAL SECURITY POLICY
- EQUAL OPS AND ETHICS POLICY
- CE HEALTH & SAFETY AND RISK ASSESSMENT POLICY

1.4 RESPONSIBILITIES

The management of **CALEDONIAN ENGLISH** create and review this policy.

The Information Security Manager facilitates the implementation of this policy through the appropriate standards and procedures.

All personnel and contracted suppliers follow the procedures to maintain the information security policy.

All personnel have a responsibility for reporting security incidents and any identified weaknesses.

Any deliberate act to jeopardise the security of information that is the property of **CALEDONIAN ENGLISH** or their customer or suppliers will be subject to disciplinary and/or legal action as appropriate.

Review

The policy is reviewed bi-annually and in case of influencing changes to ensure it remains appropriate for the business and our ability to serve our customers.

Signed

Director and Centre Manager: David MacFarlane

Date: 03/02/2020

2 ACCEPTABLE USE POLICY

Overview

Infosec's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to CALEDONIAN ENGLISH's established culture of openness, trust and integrity. Infosec is committed to protecting CALEDONIAN ENGLISH's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of CALEDONIAN ENGLISH. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every CALEDONIAN ENGLISH employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at CALEDONIAN ENGLISH. These rules are in place to protect the employee and CALEDONIAN ENGLISH. Inappropriate use exposes CALEDONIAN ENGLISH to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct CALEDONIAN ENGLISH business or interact with internal networks and business systems, whether owned or leased by CALEDONIAN ENGLISH, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at CALEDONIAN ENGLISH and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with CALEDONIAN ENGLISH policies and standards, and local laws and regulation. Exceptions to this policy are documented in section 5.2

This policy applies to employees, contractors, consultants, temporaries, and other workers at CALEDONIAN ENGLISH, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by CALEDONIAN ENGLISH.

2.1 POLICY

2.2 GENERAL USE AND OWNERSHIP

- CALEDONIAN ENGLISH proprietary information stored on electronic and computing devices whether owned or leased by CALEDONIAN ENGLISH, the employee or a third

party, remains the sole property of CALEDONIAN ENGLISH. You must ensure through legal or technical means that proprietary information is protected in accordance with the EU Data Protection Standard GDPR: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations_en.

- You have a responsibility to promptly report the theft, loss or unauthorized disclosure of CALEDONIAN ENGLISH proprietary information.
- You may access, use or share CALEDONIAN ENGLISH proprietary information only to the extent it is authorized and necessary to fulfil your assigned job duties.
- Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
- For security and network maintenance purposes, authorised individuals within CALEDONIAN ENGLISH may monitor equipment, systems and network traffic at any time, per Infosec's Audit Policy.
- CALEDONIAN ENGLISH reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

2.3 Security and Proprietary Information

- All mobile and computing devices that connect to the internal network must comply with the Minimum Access Policy.
- System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
- All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.
- Postings by employees from a CALEDONIAN ENGLISH email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of CALEDONIAN ENGLISH, unless posting is in the course of business duties.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

2.4 UNACCEPTABLE USE

- The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).
- Under no circumstances is an employee of CALEDONIAN ENGLISH authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing CALEDONIAN ENGLISH-owned resources.
- The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

2.5 SYSTEM AND NETWORK ACTIVITIES

- The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by CALEDONIAN ENGLISH.
2. Unauthorised copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which CALEDONIAN ENGLISH or the end user does not have an active license is strictly prohibited.
3. Accessing data, a server or an account for any purpose other than conducting CALEDONIAN ENGLISH business, even if you have authorized access, is prohibited.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
7. Using a CALEDONIAN ENGLISH computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
8. Making fraudulent offers of products, items, or services originating from any CALEDONIAN ENGLISH account.

9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

11. Port scanning or security scanning is expressly prohibited unless prior notification to Infosec is made.

12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

13. Circumventing user authentication or security of any host, network or account.

14. Introducing honeypots, honeynets, or similar technology on the CALEDONIAN ENGLISH network.

15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

17. Providing information about, or lists of, CALEDONIAN ENGLISH employees to parties outside CALEDONIAN ENGLISH.

2.6 Email and Communication Activities

- When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

3. Unauthorized use, or forging, of email header information.

4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

6. Use of unsolicited email originating from within CALEDONIAN ENGLISH's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by CALEDONIAN ENGLISH or connected via CALEDONIAN ENGLISH's network.

7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

2.7 Blogging and Social Media

1. Blogging by employees, whether using CALEDONIAN ENGLISH's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of CALEDONIAN ENGLISH's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate CALEDONIAN ENGLISH's policy, is not detrimental to CALEDONIAN ENGLISH's best interests, and does not interfere with an employee's regular work duties. Blogging from CALEDONIAN ENGLISH's systems is also subject to monitoring.

2. CALEDONIAN ENGLISH's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any <Company> confidential or proprietary information, trade secrets or any other material covered by <Company>'s Confidential Information policy when engaged in blogging.

3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of CALEDONIAN ENGLISH and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by CALEDONIAN ENGLISH's *Non-Discrimination and Anti-Harassment* policy.

4. Employees may also not attribute personal statements, opinions or beliefs to CALEDONIAN ENGLISH when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of CALEDONIAN ENGLISH. Employees assume any and all risk associated with blogging.

5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, CALEDONIAN ENGLISH's trademarks, logos and any

other CALEDONIAN ENGLISH intellectual property may also not be used in connection with any blogging activity.

3 CLEAN DESK POLICY

Overview

A clean desk policy can be an import tool to ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or an employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace. Such a policy can also increase employee's awareness about protecting sensitive information.

Purpose

The purpose for this policy is to establish the minimum requirements for maintaining a "clean desk" – where sensitive/critical information about our employees, our intellectual property, our customers and our vendors is secure in locked areas and out of site. A Clean Desk policy is not only ISO 27001/17799 compliant, but it is also part of standard basic privacy controls.

Scope

This policy applies to all CALEDONIAN ENGLISH employees and affiliates.

3.1 POLICY

3.2 REQUIREMENTS

1. Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
2. Computer workstations must be locked when workspace is unoccupied.
3. Computer workstations must be shut completely down at the end of the work day.
4. Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.
5. File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
6. Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.
7. Laptops must be either locked with a locking cable or locked away in a drawer.
8. Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
9. Printouts containing Restricted or Sensitive information should be immediately removed from the printer.

10. Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.
11. Whiteboards containing Restricted and/or Sensitive information should be erased.
12. Lock away portable computing devices such as laptops and tablets.
13. Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer
14. All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

4 ROUTER AND SWITCH SECURITY POLICY

Overview

See Purpose.

Purpose

This document describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of CALEDONIAN ENGLISH.

Scope

All employees, contractors, consultants, temporary and other workers at CALEDONIAN ENGLISH and its subsidiaries must adhere to this policy. All routers and switches connected to CALEDONIAN ENGLISH production networks are affected.

4.1 POLICY

4.2 EVERY ROUTER MUST MEET THE FOLLOWING CONFIGURATION STANDARDS:

1. No local user accounts are configured on the router. Routers and switches must use TACACS+ for all user authentication.
2. The enable password on the router or switch must be kept in a secure encrypted form. The router or switch must have the enable password set to the current production router/switch password from the device's support organization.
3. The following services or features must be disabled:
    a. IP directed broadcasts
    b. Incoming packets at the router/switch sourced with invalid addresses such as RFC1918 addresses
    c. TCP small services
    d. UDP small services
    e. All source routing and switching
    f. All web services running on router

g. CALEDONIAN ENGLISH discovery protocol on Internet connected interfaces

h. Telnet, FTP, and HTTP services

i. Auto-configuration

4. The following services should be disabled unless a business justification is provided:

    a. CALEDONIAN ENGLISH discovery protocol and other discovery protocols

    b. Dynamic trunking

    c. Scripting environments, such as the TCL shell

5. The following services must be configured:

    a. Password-encryption

    b. NTP configured to a corporate standard source

6. All routing updates shall be done using secure routing updates.

7. Use corporate standardized SNMP community strings. Default strings, such as public or private must be removed. SNMP must be configured to use the most secure version of the protocol allowed for by the combination of the device and management systems.

8. Access control lists must be used to limit the source and type of traffic that can terminate on the device itself.

9. Access control lists for transiting the device are to be added as business needs arise.

10. The router must be included in the corporate enterprise management system with a designated point of contact.

11. Each router must have the following statement presented for all forms of login whether remote or local:

    "UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right

to privacy on this device. Use of this system shall constitute consent to monitoring."

12. Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSH version 2 is the preferred management protocol.
13. Dynamic routing protocols must use authentication in routing updates sent to neighbors. Password hashing for the authentication string must be enabled when supported.
14. The corporate router configuration standard will define the category of sensitive routing and switching devices, and require additional services or configuration on sensitive devices including:
    a. IP access list accounting
    b. Device logging
    c. Incoming packets at the router sourced with invalid addresses, such as RFC1918 addresses, or those that could be used to spoof network traffic shall be dropped
    d. Router console and modem access must be restricted by additional security controls

5 PASSWORD PROTECTION POLICY

Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of our resources. All staff, including contractors and vendors with access to CALEDONIAN ENGLISH systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

The purpose of this policy is to establish a standard for creation of strong passwords and the protection of those passwords.

Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any CALEDONIAN ENGLISH facility, has access to the CALEDONIAN ENGLISH network, or stores any non-public CALEDONIAN ENGLISH information.

5.1 POLICY

5.2 PASSWORD CREATION

1 All user-level and system-level passwords must conform to the Password Construction Guidelines.

2 Users must use a separate, unique password for each of their work related accounts. Users may not use any work related passwords for their own, personal accounts.

3 User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges. In addition, it is highly recommend that some form of multi-factor authentication is used for any privileged accounts

5.3 Password Change

- Passwords should be changed only when there is reason to believe a password has been compromised.
- Password cracking or guessing may be performed on a periodic or random basis by the Infosec Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.

5.4 Password Protection

- Passwords must not be shared with anyone, including supervisors and co-workers. All passwords are to be treated as sensitive, Confidential CALEDONIAN ENGLISH information. Corporate Information Security recognizes that legacy applications do not support proxy systems in place. Please refer to the technical reference for additional details.
- Passwords must not be inserted into email messages, Alliance cases or other forms of electronic communication, nor revealed over the phone to anyone.
- Passwords may be stored only in “password managers” authorized by the organization.
- Do not use the "Remember Password" feature of applications (for example, web browsers).
- Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

5.5 Application Development

Application developers must ensure that their programs contain the following security precautions:

- Applications must support authentication of individual users, not groups.
- Applications must not store passwords in clear text or in any easily reversible form.
- Applications must not transmit passwords in clear text over the network.
- Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

5.6 Multi-Factor Authentication

- Multi-factor authentication is highly encouraged and should be used whenever possible, not only for work related accounts but personal accounts also.

6 DATA BREACH RESPONSE POLICY

Purpose

The purpose of the policy is to establish the goals and the vision for the breach response process. This policy will clearly define to whom it applies and under what circumstances, and it will include the definition of a breach, staff roles and responsibilities, standards and metrics (e.g., to enable prioritization of the incidents), as well as reporting, remediation, and feedback mechanisms. The policy shall be well publicized and made easily available to all personnel whose duties involve data privacy and security protection.

CALEDONIAN ENGLISH Information Security's intentions for publishing a Data Breach Response Policy are to focus significant attention on data security and data security breaches and how CALEDONIAN ENGLISH's established culture of openness, trust and integrity should respond to such activity. CALEDONIAN ENGLISH Information Security is committed to protecting CALEDONIAN ENGLISH's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Background

This policy mandates that any individual who suspects that a theft, breach or exposure of CALEDONIAN ENGLISH Protected data or CALEDONIAN ENGLISH Sensitive data has occurred must immediately provide a description of what occurred via e-mail to INFO@CALEDONIANENGLISH.COM, by calling +393880538561, or through the use of the web page at http://caledonianenglish.com. This e-mail address, phone number, and web page are monitored by the CALEDONIAN ENGLISH's Information Security Administrator. This team will investigate all reported thefts, data breaches and exposures to confirm if a theft, breach or exposure has occurred. If a theft, breach or exposure has occurred, the Information Security Administrator will follow the appropriate procedure in place.

Scope

This policy applies to all whom collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifiable information or Protected Health Information (PHI) of CALEDONIAN ENGLISH members. Any agreements with vendors will contain language similar that protects the fund.

6.1 POLICY

6.2 CONFIRMED THEFT, DATA BREACH OR EXPOSURE OF CALEDONIAN ENGLISH PROTECTED DATA OR CALEDONIAN ENGLISH SENSITIVE DATA

- As soon as a theft, data breach or exposure containing CALEDONIAN ENGLISH Protected data or CALEDONIAN ENGLISH Sensitive data is identified, the process of removing all access to that resource will begin.
- The Centre Director will handle the breach or exposure and advise all parties affected.

6.3 CONFIRMED THEFT, BREACH OR EXPOSURE OF CALEDONIAN ENGLISH DATA

The Centre Director will be notified of the theft, breach or exposure. IT, along with the designated forensic team, will analyse the breach or exposure to determine the root cause.

6.4 WORK WITH FORENSIC INVESTIGATORS

As provided by CALEDONIAN ENGLISH cyber insurance, the insurer will need to provide access to forensic investigators and experts that will determine how the breach or exposure occurred; the types of data involved; the number of internal/external individuals and/or organizations impacted; and analyse the breach or exposure to determine the root cause.

6.5 DEVELOP A COMMUNICATION PLAN.

Work with CALEDONIAN ENGLISH communications, legal and human resource departments to decide how to communicate the breach to: a) internal employees, b) the public, and c) those directly affected.

6.6 OWNERSHIP AND RESPONSIBILITIES

6.7 ROLES & RESPONSIBILITIES:

- Sponsors - Sponsors are those members of the CALEDONIAN ENGLISH community that have primary responsibility for maintaining any particular information resource. Sponsors may be designated by any CALEDONIAN ENGLISH Executive in connection with

their administrative responsibilities, or by the actual sponsorship, collection, development, or storage of information.

- Information Security Administrator is that member of the CALEDONIAN ENGLISH community, designated by the Centre Director or the Director, Information Technology (IT) Infrastructure, who provides administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources in consultation with the relevant Sponsors.
- Users include virtually all members of the CALEDONIAN ENGLISH community to the extent they have authorized access to information resources, and may include staff, trustees, contractors, consultants, interns, temporary employees and volunteers.
- The Incident Response Team shall be chaired by Executive Management and shall include, but will not be limited to, the following departments or their representatives: IT-Infrastructure, IT-Application Security; Communications; Legal; Management; Financial Services, Member Services; Human Resources.

6.8 ENFORCEMENT

- Any CALEDONIAN ENGLISH personnel found in violation of this policy may be subject to disciplinary action, up to and including termination of employment.

- Any third-party partner company found in violation may have their network connection terminated.