POLICY DOCUMENT

Information Security Policy

Document no:	7.0.2023
Version:	9.0
Responsible:	Vice President of Systems Technology
Approved by the Board of Directors on:	4th December 2023

Table of Contents

1. BACKGROUND AND PURPOSE

This Information Security Policy (the "**Policy**") for Catena Media Plc. (the "**Company**") and its subsidiaries (jointly referred to as the "**Catena Group**") has been developed to ensure that the Catena Group conducts business with integrity, while ensuring confidentiality and availability of information, the supporting IT systems, business processes, and personal data.

The Vice President of Systems Technology is ultimately responsible for ensuring the rules and principles in this Policy are adhered to. Strategic information security decisions in the Catena Group shall be made by the Vice President of Systems Technology, supported by advice from the members of the management team

2. AUDIENCE

This Policy applies to all directors, employees (including interns, apprentices, trainees, and third party hired), independent contractors, founders on earn-out and other similarly contracted workers (collectively known as "**Relevant Persons**").

3. COMPANY PREMISES ACCESS

Each office should secure the premise using an access control system where the staff will be issued security access cards to access the premises. The available hours should be predefined and any deviations from the default hours should be signed off by the Information Security team. For further information, please see the company premises access procedure.

4. INTERNET ACCESS

The Internet provides resources that are essential to the success of our business. However, it is also the primary source of uncontrolled, inappropriate, and malicious content, which could cause significant harm to our continued operations. It is for this reason that all Internet access using company assets is controlled by Corporate IT and governed by the Information Security team where available, through the web filter policies in the firewall to block the malicious content mentioned in "4.1".

These policies block:

- Potentially liable content
- Adult content
- Peer-to-peer networks
- Sites deemed as security risks

All systems activity is monitored by monitoring software which is installed and maintained by the Tech Operations department. The software monitoring for malicious content, inappropriate use viruses and software with malicious intent (malware).

When working remotely all Relevant Persons must use the Company's approved VPN service provider or approved access control services. This is to ensure that all activity passes through the necessary checks for it not to be deemed suspicious or malicious. In fact, the use of VPN and or approved access control services will allow you to perform your job duties without the risk of having a security control interrupting your work.

4.1 MALICIOUS CONTENT AND INAPPROPRIATE USE

Examples of malicious content and inappropriate Internet use include access and browsing of websites and discussion groups that contain the following types of content:

- Drugs, and Adult Material
- Military, Extremist Views and Weapons
- Inciting Racism, Hate and Violence
- Computer Hacking, Viruses Propagation and Malicious Code
- Illegal and Unlicensed Software, Films and Music

Exemptions to the above are granted in certain limited circumstances and only following Information Security approval.

4.2 COMPUTER VIRUSES AND SOFTWARE WITH MALICIOUS INTENT (MALWARE)

Malware is a significant threat to computer systems and could cause damage and disruption to business activities. Catena Group implements security controls and technology to help protect and react to different types of malware including viruses.

Prevention against virus infection is our best defense therefore, it is important we adhere to the following:

- Virus contamination or infection warnings from your computer must be reported immediately
- Storage devices, disks and media received from any external source or networks must be virus checked prior to use
- Only open email file attachments, compressed and encrypted files from trusted sources
- Do not send or receive executable application files by email
- Only use the business Google Drive for file storage which is connected with the Company's Google Workspace account
- Do not open suspicious email from unknown sources When in doubt, reach out to Information Security at security@catenamedia.com for assistance

Catena Group employs Bitdefender as the only accepted anti-malware software. The anti-malware software is a requirement and must be installed on all company devices globally and shall not be removed by the employee.

4.3 PHISHING

Phishing is an attempt to gather information from unsuspecting individuals that they would otherwise never disclose. Phishing is an effective tool used by attackers to deceive people and acquire information such as usernames, passwords, bank account details and credit card details without prior leads. Phishing attacks can take place over a number of platforms, including but not limited to the ones listed below:

- Email
- WhatsApp
- Text
- Slack
- Phone call
- Skype

Often these attacks include links to web sites, data entry forms, computer viruses and malicious code; on the surface, they can look genuine and trustworthy. Phishing is the most common attack vector used by hackers to target Catena Group.

The business deploys security controls to identify, capture and stop these types of attacks on Company approved methods of communication, it also conducts routine anti-phishing hands-on training to equip its staff with the best knowledge to stop these kinds of attacks. Despite all of these efforts, phishing attempts may still get through so it is important that one must always be able to confirm the legitimacy of who they are communicating with. If you suspect you are being targeted by an attempted phishing attack, you should raise the suspicious communication effort with security via the phishing email address: phishing@catenamedia.com as quickly as possible to ensure a quick, effective and orderly investigation and response.

5. CONFIDENTIAL, SENSITIVE AND PERSONAL DATA

The information we process in the daily course of business contains confidential, sensitive, and personal data (jointly referred to as the "**Information**"). It is important that all staff handles, stores, and disposes of the Information securely. This includes physical and digital assets.

Failure to handle the Information appropriately may cause operational issues, difficulty in protecting our customers' interests and reputational damage through unauthorized or accidental disclosure outside of the business.

All sensitive information and personal data should be encrypted whilst being handled, transmitted and stored.

5.1 HANDLING AND STORING THE INFORMATION

The Catena Group employs Google Drive as the only accepted system for cloud file storage. All Relevant Persons must use the Google Drive facilities provided by the Tech Operations department. Exemptions may be granted in certain limited circumstances. Additional cloud storage can be granted by Tech Operations Department only for legitimate business needs.

When using cloud-based storage, all Relevant Persons are required to protect the integrity and confidentiality of Information (as defined below) contained in business documents or files. Information must be shared on a strictly need to know basis and relevant security, access, and confidentiality settings must be implemented. Periodically, all Relevant Persons must review and audit the Information accessible in their individual and/or shared drives and delete any Information and/or remove any accesses that are no longer needed. Files and folders, especially those containing personal data, should be named appropriately and uniquely for ease of management and discovery.

With regards to physical (non-digital) Information, this can be stored in designated secure drawers and/or safes (paper-based) and only shared via the email facilities provided by the Catena Group and not via other work tools (e.g. Slack) or via whiteboards and any other surfaces used for sketching and notes. Information in paper-based form shall be limited to what is necessary or required.

Information should **NOT** be:

- Published or circulated internally to staff that do not require access to perform their role
- Sent to, exchanged with, or disclosed to a third party without a formal non-disclosure agreement and/or Data Processing Agreement
- Transmitted over public networks without strong cryptography and relevant security protocols
- Sent over any form of communication which is not approved by the Company.
- Stored on devices and accompanying media that fit the following device classifications:
    - Portable USB-based memory sticks, flash drives, or thumb drives, jump drives, or key drive
    - Memory cards in SD, CompactFlash, Memory Stick, or any related flash-based supplemental storage media
    - USB card readers that allow connectivity to a PC or laptop
    - Portable MP3 and MPEG-playing music and media player-type devices such as iPods with internal flash or hard drive-based memory that support a data storage function
    - Cell phone handsets, and smartphones with internal flash or hard drive-based memory that support a data storage function
    - Digital cameras with internal or external memory support
    - Removable memory-based media, such as rewritable DVDs, CDs, and floppy disks Any hardware that provides connectivity to USB devices through means such as wireless (WiFi, WiMAX, irDA, Bluetooth, among others) or wired network access

- Cloud based storage services that are not linked to a Company approved email address
- Any other hardware and related software that could be used to access the Catena Group resources

- For the avoidance of doubt, the use of all hardware and software listed above is strictly prohibited to all Relevant Persons. Exemptions may be granted in certain limited circumstances otherwise approved by the Information Security team.
- Put into the general waste for disposal, make sure that the documents are shredded before disposal
- Kept for longer than is necessary or disposed of prior to the allocated retention period

At the end of a workday, work laptops or PCs must be shut down completely.

When a workstation is unattended, the account must be locked so as to avoid access by unauthorised parties. This can easily be done by pressing the Windows + L keys on all windows devices or by pressing Command + Q on an Apple device.

All Information in paper form must not be left unattended (e.g. post-it notes on desks) and must be locked in a safe drawer/cabinet. Such drawers/cabinets must be kept closed and locked at all times. Access to such drawers/cabinets must also be limited to only those individuals who need access in order to fulfil their day-to-day business.

When printing documents containing sensitive Information, you must use a secure printing function, not leave the printer unattended, and remove any documents from the printer tray once printed.

Further, personal data must be also handled and stored in accordance with the principles and rules set out in the Company's Data Protection Policy.

5.2 DISPOSAL OF THE INFORMATION

Information in electronic form must be disposed of as soon as no longer necessary Personal data must be kept in accordance with the principles set out in the Company's Data Protection Policy.

Paper-based Information must be disposed via shredding.

6. EMAIL FACILITIES

Email facilities are provided by the business as an essential communication tool and must be used appropriately for business purposes only. In the daily course of business all Relevant Persons must use the email facilities provided by the business; usage of personal email is strictly prohibited. All internal, inbound, and outbound email communications are stored in accordance with the Catena Group Employee Privacy Notice.

7. COMPUTER HARDWARE AND SOFTWARE

The use of unauthorized hardware is not permitted. All Relevant Persons must only use Company approved equipment which has been configured to Company standards.

The use of unsecured network connections is not permitted. Refer to section 4 for information regarding use of Company VPN.

Relevant persons making use of mobile phones or tablets for work related tasks are expected to be aware of the risks involved and should follow best security practices mentioned within this policy when doing so.

All IT equipment and connections to the computer network must be authorized by the Tech Operations department. All IT hardware and software purchases must therefore be handled by the Tech Operations department and, when involving personal data, must be in line with the Privacy by Design and by Default Procedure and New Processor Procedure. All Relevant Persons are responsible for consulting with the Tech Operations department when contemplating such a purchase.

If you take equipment off-site, you are responsible for its safe return. The unauthorized disposal of IT equipment is not permitted. The disposal of computer equipment must follow the standard procedure to protect the business from any unauthorized or accidental security incident.

When using IT equipment, you must ensure that you:

- Do not leave your work laptop unattended
- Lock your computer screen when you are not at your desk
- Do not connect any unauthorized or personal equipment to your terminal or computer
- Ensure you logout from any application or network services no longer needed

The copying, downloading, distributing or use of unauthorized, copyright protected, illegal software is prohibited.

Software licensing law mandates that the business retains and manages all software licensing and original media in a diligent manner for the duration of the ownership to reduce the risk of installing and using unlicensed software and applications.

8. IT SYSTEM ACCESS AND PASSWORDS

Passwords are used to help control access to our IT systems and information by providing an extra layer of defense against unauthorized access. They are unique to each individual user and as such must not be divulged to anyone. Passwords must be changed if there is any indication of their possible compromise.

The first time you log on to a system, you will be automatically asked to change your password immediately. In the case where systems do not offer this feature you are duty bound to change the password manually after logging in.

It is important you choose a strong and unique password that has never been breached. Passwords must be created in accordance with the rules set out in the Company's Password Procedure.

If you have more than one password for access to multiple systems or applications, it is a requirement that you use a different password for each account. This approach will provide enhanced security and the longer the length of your password the harder to predict.

Password use is controlled and monitored by the Tech Operations Department, consequently:

- 1Password should be used for access and storing passwords to all systems
- After your first successful logon, you can change your password at any time
- Your password can be reset by the Tech Operations Department

Passwords must be stored securely, and not be left on sticky notes, posted on or under a computer/laptop, nor may they be left written down in an accessible location.

9. BACKUP OF INFORMATION

The Tech Operations department backup all business information to a centrally provisioned service on a regular basis. This is to ensure that any disruption of business activities due to data loss, data corruption, system failures or accidental deletion can be recovered and restored back to operational efficiency in a timely manner.

For this reason, all business information and data must be saved to and stored on the file shares, data repositories, databases and applications provided to individuals to support business operations. Information must not be saved or stored in locations that are not subject to regular scheduled backup procedures.

Individuals provisioned with laptop computers that allow for the local storage of data must:

- Ensure regular data synchronization with network file shares or Catena Group Google Drive to ensure business data is backed up
- Not backup data to their personal devices or home computer systems

10. SECURITY INCIDENT REPORTING

Security incidents can have an adverse effect on business processes and may cause damage to the Company's assets, information, and reputation. Security incidents, events and unusual behavior of IT systems must be reported to the Information Security team as quickly as possible to ensure a quick, effective, and orderly response.

Examples of security incidents or events include (but not limited to) the following:

- Breaches of this Policy
- Virus contamination or infection warnings

- Unsolicited or offensive “Spam” emails or telephone calls
- Theft of equipment
- Loss of paper files or equipment outside of the business premises
- Unauthorized disclosure of information, passwords, or suspected password weaknesses
- Ineffective security control
- Malfunctions of software or hardware
- Access violations
- Unaccounted system changes
- Breaches of physical security arrangements
- Breaches on integrity, confidentiality or availability expectations
- Breaches of personal data

When you suspect a security incident, events or unusual behavior of IT systems do not attempt to:

- Remedy any IT equipment malfunctions or failures
- Remove or fix virus and malware infections
- React to security incidents or perform unauthorized investigation

Security incidents, events and unusual behavior of IT systems must be reported as soon as possible to the Information Security team, no later than 24h of a Relevant person becoming aware, and must be documented and dealt with in accordance with the guidelines set out in the Company’s Security Incident Managing Procedure or Personal Breach Procedure, as applicable.

11. EMPLOYEE OFFBOARDING

Employee departures may result in the loss of property or information if they are not handled properly. Well-developed offboarding procedures help mitigate the risks of those transitions by outlining appropriate roles and responsibilities. An employee will be entered into the Offboarding Jira board by the HR business partner when a final date has been agreed upon following resignation.

The Human Resources department will coordinate the transfer of all Company property prior to an employee’s departure with the Tech Operations department. The departing employee will be responsible for returning all Company property in acceptable condition. A departing employee must also identify and transfer all Company’s electronic resources, access, and documents.

The Tech Operations department will revoke all access to the Company's systems and building upon an employee’s departure.

Upon departure an employee should conduct an exit interview with HR.

12. ROLES AND RESPONSIBILITIES

All Relevant Persons are individually responsible for ensuring their adherence to this Policy.

The Vice President of Systems Technology is responsible for reviewing and updating this Policy.

The CEO is the overall owner of this Policy.

13. REVIEWS AND UPDATES

The Information Security Policy shall be reviewed, updated, and adopted when deemed necessary or appropriate, however, no less than annually.

The Information Security Policy shall be reviewed and updated by the Vice President of Systems Technology and adopted by the Board of Directors.

14. REFERENCES TO ASSOCIATED DOCUMENTS

- Password Procedure
- Security Incident Management Procedure
- Data Protection Policy
- Company Premises Access Procedure