POLICY DOCUMENT

Information Security Policy

Document no:	7.0.2025
Version:	10.0
Responsible:	Chief Technical Officer
Approved by the Board of Directors on:	19th November 2025

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 Chief Technical Officer ("CTO") holds ultimate responsibility for ensuring adherence to the rules and principles outlined in this Policy. Strategic information security decisions within the Catena Group will be made by the CTO, supported by the Head of Information Security.

2. AUDIENCE

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

3. PHYSICAL ACCESS - COMPANY PREMISES

To ensure the security and integrity of Catena Media's physical assets and facilities, this policy governs the management of physical access and protects the organisation's premises from unauthorised entry or damage. This is crucial for safeguarding sensitive information, supporting IT systems, and maintaining business operations.

- Access Control Measures:
    - Employees must use company-issued access cards, while visitors and third parties are issued temporary access credentials. Role-Based Access Control (RBAC) ensures that access is granted based on individual responsibilities.
- Monitoring and Logging:
    - CCTV systems monitor entry and exit points, and all access events are logged to maintain an audit trail. Employees must wear visible identification badges at all times, and visitors must be escorted by authorised personnel within Catena Media's premises.
- Roles and Responsibilities:
    - The policy defines clear responsibilities for key personnel, including the CTO, Head of Information Security, HR, and Office Manager, among others, ensuring coordinated efforts in maintaining physical security.
- Enforcement and Compliance:
    - Compliance with this policy is mandatory, with disciplinary actions for violations. Regular audits and risk assessments are conducted to identify and mitigate physical security risks.
- Accounts Governance:
    - All accounts must include all required labels as mandated in the Access procedure.

- All accounts must be assigned to an owner responsible for the account's lifecycle.

Further details are provided in the Physical 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

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 defence 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 Microsoft Onedrive and Sharepoint for file storage which is connected with the Company's Microsoft account
- Do not open suspicious emails from unknown sources. When in doubt, reach out to Information Security at security@catenamedia.com for assistance

Catena Group employs Crowdstrike 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.

In limited circumstances, exemptions to these restrictions may be granted. Prior to accessing any content that is normally prohibited under this policy, approval must be obtained from Information Security.

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. The business 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 unauthorised 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 Microsoft Onedrive and Sharepoint as the only accepted system for cloud file storage. All Relevant Persons must use the Microsoft suite facilities provided by the Tech Operations department. Exemptions may be granted in certain limited circumstances. Additional cloud storage can be granted by the 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 company-approved.
    - 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.

Documents stored in in-scope systems (Microsoft Onedrive and Sharepoint as specified in 5.1 Handling and Storing the Information) must be labelled to identify the information they contain. Related security controls will be implemented within these systems to ensure secure handling and processing of data. Details on the different labels, their usage, and data handling requirements can be found in the Data Classification and Handling Procedure. Alternate systems must not be used to circumvent these security controls unless it is not possible to use Microsoft Suite. In such cases, it is expected that the user ensures data is handled securely.

Further, personal data must also be 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 of 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 unauthorised hardware is not permitted. All Relevant Persons must only use Company approved equipment which has been configured to Company standards.

Limited private use is permitted but only in accordance with the Company's Information Security Policy and communicated restrictions on the use of personal devices. 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 Company instructions and best security practices mentioned within this policy and the Company's Code of Conduct when doing so.

All IT equipment and connections to the computer network must be authorised 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, it must meet the requirements mandated by the Legal and Privacy teams. 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 unauthorised disposal of IT equipment is not permitted. The disposal of computer equipment must follow the standard procedure to protect the business from any unauthorised 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 unauthorised or personal equipment to your terminal or computer
- Ensure you logout from any application or network services that are no longer needed

The copying, downloading, distributing or use of unauthorised, 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 defence against unauthorised 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.

Further details on selection and handling of password can be found in the Password Procedure.

9. BACKUP OF INFORMATION

The company regularly backs up all business information to a centrally provisioned service to ensure that any disruption of business activities due to data loss, data corruption, system failures, or accidental deletion can be recovered and restored 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 synchronisation with network file shares or Catena Group Onedrive and Sharepoint to ensure business data is backed up.
- Not backup data to their personal devices, other non-approved cloud service providers 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
- Unauthorised 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 behaviour 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 unauthorised investigation

Security incidents, events and unusual behaviour 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 Management Procedure.

Use the designated Jira Service Desk to log all details related to the security incident. Include information such as the nature of the incident, the time it was detected, and any immediately apparent impacts.

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 and within the timeframe specified by the Company. 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. ASSET MANAGEMENT

The Asset Management section of this Information Security Policy outlines the responsibilities and main controls for managing all assets owned or controlled by Catena Group. The goal is to ensure the appropriate protection, use, and management of the company's physical, digital, and intellectual assets to maintain business continuity, security, and compliance.

PURPOSE

This section aims to establish a structured approach for the identification, acquisition, maintenance, and disposal of all assets within the organisation, covering hardware, software, data, and intellectual property. This helps reduce risks, ensures proper use, and supports compliance with applicable regulations and standards.

MAIN CONTROLS

- **Asset Inventory and Ownership**: A centralised inventory of all assets must be maintained, with each asset assigned an owner responsible for managing its lifecycle.
- **Tagging and Labelling**: All assets must be tagged and classified according to their criticality, with periodic reviews to ensure the classification is accurate. Assets containing sensitive data must be labelled appropriately.
- **Handling and Protection**: Secure handling procedures must be followed to protect assets from unauthorised access, modification, or destruction. Sensitive data must be encrypted, and physical assets must be stored securely.
- **Asset Maintenance and Lifecycle Management**: Assets must be managed throughout their lifecycle, from acquisition to secure disposal. Regular audits must be conducted to verify asset inventory accuracy and identify potential improvements.
- **Roles and Responsibilities**: Specific roles are defined for Asset Owners, IT Department, and Employees to ensure accountability for asset management.

Further details can be found in the Asset Management Procedure.

13. ROLES AND RESPONSIBILITIES

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

The Chief Technology Officer is responsible for reviewing and updating this Policy.

The Head of Information Security is responsible for implementing the information security policy, managing daily security operations, ensuring compliance, leading the security team, and reporting on security status to the Chief Technology Officer.

The CEO is the overall owner of this Policy.

14. 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 Chief Technology Officer and adopted by the Board of Directors.

15. REFERENCES TO ASSOCIATED DOCUMENTS

- Data Protection Policy
- Information Security Governance Hub

16. Enforcement

This policy, along with all associated procedures, is mandatory and enforced across the organisation. All employees, contractors, and third-party users are required to comply fully with the standards outlined within this document. Compliance will be monitored and managed by the IT and Security departments, and any breaches of this policy may result in disciplinary action, up to and including termination of employment or contract. Regular audits and reviews will ensure adherence, and non-compliance will be addressed promptly to uphold organisational security standards.

17. Exception to the Policy

- Any **exceptions** to this policy or related procedures and standards must be reported to the **Information Security (InfoSec) Team** using the designated Jira Policy Exception form.
- The Info-Sec team will review the exception request and guide how to proceed in line with internal policy exceptions.