MERIDIA
INTERACTIVE SOLUTIONS

5 Great Valley Parkway, Suite 218, Malvern, PA 19355
Phone: 610-260-6800, Fax: 610-260-6810, Email: rsvp@meridiaars.com

Photo Communications Corp. DBA Meridia Audience Response

Information Security Policy

Last Update: 3/15/2022

1. Purpose

The purpose of this Policy is to safeguard information stored within the local facilities, and in a secure, offsite environment of the CloudVOTE Content Management System (“CloudVOTE”) by anyone who engages with Photo Communications Corp. DBA Meridia Audience Response (“Meridia”, “Company”) and becomes a Paying Client (“Client”).

This Policy informs the Client and others entitled to use CloudVOTE services that it is the goal of Meridia that:

- Information will be protected against unauthorized access or misuse.
- Confidentiality of information will be secured.
- Integrity of information will be maintained.
- Availability of information / information systems is maintained for service delivery.
- Business continuity planning processes will be maintained.
- Regulatory, contractual and legal requirements will be complied with.
- Physical, logical, environmental and communications security will be maintained.
- Infringement of this Policy may result in disciplinary action or criminal prosecution.
- When information is no longer of use, it is disposed of in a suitable manner.
- All information security incidents will be reported to the responsible party and investigated through the appropriate management channel.

Information relates to:

- Electronic information systems (software, computers, and peripherals) owned by the Company.
- The Company's computer network used either directly or indirectly.
- Hardware, software and data owned by the Company.
- Paper-based materials.
- Electronic materials, files and other data in electronic format including, but not limited to screenshots, snippets, edited or identical copies and duplicates of said materials.
- Electronic recording devices (video, audio, CCTV systems).

2. The Policy

Meridia requires all users to exercise a duty of care in relation to the operation and use of its information systems.

2.1 Authorized users of information systems

With the exception of information published for public consumption, all users of Meridia's information systems must be formally authorized by appointment as a member of staff, Client, or by other process specifically authorized in a written, individual Agreement. Authorized users will be in possession of a unique user identity. Any password associated with a user identity must not be disclosed to any other person. The "Network Password Policy" section describes these principles in greater detail.

Authorized users will pay due care and attention to protect Meridia's information in their personal possession. Confidential, personal or private information must not be copied or transported without consideration of:

- permission of the information owner
- the risks associated with loss or falling into the wrong hands
- how the information will be secured during transport and at its destination.

2.2 Acceptable use of information systems

Use of the Meridia's information systems by authorized users will be lawful, honest and decent and shall have regard to the rights and sensitivities of other people. The detail of acceptable use in specific areas may be found in the list of subsidiary policies detailed in the Appendix.

2.3 Information System Owners

Meridia employees and contractors who are responsible for information systems are required to ensure that:

1. Systems are adequately protected from unauthorized access.
2. Systems are secured against theft and damage to a level that is cost-effective.
3. Adequate steps are taken to ensure the availability of the information system, commensurate with its importance (Business Continuity).
4. Electronic data can be recovered in the event of loss of the primary source. I.e. failure or loss of a computer system. It is incumbent on all system owners to backup data and to be able to restore data to a level commensurate with its importance (Disaster Recovery).
5. Data is maintained with a high degree of accuracy.
6. Systems are used for their intended purpose and that procedures are in place to rectify discovered or notified misuse.
7. Any electronic access logs are only retained for a justifiable period to ensure compliance with the data protection, investigatory powers and freedom of information acts.
8. Any third parties entrusted with Meridia's data understand their responsibilities with respect to maintaining its security.

2.4 Personal Information

Authorized users of information systems are not given rights of privacy in relation to their use of Meridia's information systems. Duly authorized officers of the Company may access or monitor personal data contained in any Meridia information system (mailboxes, web access logs, file-store etc).

2.5 Disciplinary Procedures

Individuals in breach of this policy are subject to disciplinary procedures (staff or contractor) at the instigation of the manager or supervisor with responsibility for the relevant information system, including referral to the Police where appropriate.

Meridia will take legal action to ensure that its information systems are not used by unauthorized persons.

3. OWNERSHIP

3.1 Chief Operating Officer (COO) has direct responsibility for maintaining this policy and providing guidance and advice on its implementation.

Information system owners are responsible for the implementation of this Policy within their area, and to ensure adherence.

A. APPENDIX: SUBSIDIARY POLICIES

The detail of acceptable use in specific areas may be found in the following list of subsidiary polices:

A1 Network Password Policy

A1.1 Overview

This policy is intended to establish guidelines for effectively creating, maintaining, and protecting passwords at Meridia.

A1.2 Scope

This policy shall apply to all clients, employees, contractors, and affiliates of Meridia, and shall govern acceptable password use on all systems that connect to Meridia network or access or store Meridia, or CloudVOTE data.

A1.3 Policy

A1.3.1 Password Creation

All user and admin passwords must be at least [8] characters in length. Longer passwords and passphrases are strongly encouraged.
Where possible, password dictionaries should be utilized to prevent the use of common and easily cracked passwords.
Passwords must be completely unique, and not used for any other system, application, or personal account.
Default installation passwords must be changed immediately after installation is complete.

A1.3.2 Password Aging

User passwords must be changed every [3] months. Previously used passwords may not be reused.
System-level passwords must be changed on a quarterly basis.

A1.3.3 Password Protection

Passwords must not be shared with anyone (including co-workers and supervisors) and must not be revealed or sent electronically.
Passwords shall not be written down or physically stored anywhere in the office.
When configuring password "hints," do not hint at the format of your password (e.g., "zip + middle name")
User IDs and passwords must **not** be stored in an unencrypted format.
User IDs and passwords must **not** be scripted to enable automatic login.
"Remember Password" feature on websites and applications should not be used.

A1.3.4 Enforcement

It is the responsibility of the end user to ensure enforcement with the policies above.

If you believe your password may have been compromised, please immediately report the incident to your direct supervisor and change the password using the policy rules above.