Document Control

Organisation	Harmony Marketing Group
Title	Privacy Policy
Filename	privacypolicy.docx
Contact	Tim Harman
Title	President
Contact	574.342.0215

Privacy Policy Statement

Harmony will establish specific requirements for protecting information and information systems against unauthorised access.

Harmony will effectively communicate the need for information and information system access control.

1 Purpose

Information security is the protection of information against accidental or malicious disclosure, modification or destruction. Information is an important, valuable asset of Harmony which must be managed with care. All information has a value to the company. However, not all of this information has an equal value or requires the same level of protection.

Access controls are put in place to protect information by controlling who has the rights to use different information resources and by guarding against unauthorised use.

Formal procedures must control how access to information is granted and how such access is changed.

2 Scope

This policy applies to all Harmony Committees, Departments, Partners, and Employee with any form of access to Harmony's information and information systems.

3 Definition

Access control rules and procedures are required to regulate who can access Harmony information resources or systems and the associated access privileges. This policy applies at all times and should be adhered to whenever accessing Harmony information in any format, and on any device.

4 Risks

Individuals or companies, without the correct authorisation and clearance may intentionally or accidentally gain unauthorised access to business information which may adversely affect day to day business. This policy is intended to mitigate that risk.

Non-compliance with this policy could have a significant effect on the efficient operation of the company and may result in financial loss and an inability to provide necessary services to our customers**.**

5 Applying the Policy – Employee Access

5.1 User Access Management

Formal user access control procedures must be documented, implemented and kept up to date for each application and information system to ensure authorised user access and to prevent unauthorised access. They must cover all stages of the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access. These must be agreed by Harmony. Each user must be allocated access rights and permissions to computer systems and data that:

- Are commensurate with the tasks they are expected to perform.
- Have a unique login that is not shared with or disclosed to any other user.
- Have an associated unique password that is requested at each new login.

User access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated. System administration accounts must only be provided to users that are required to perform system administration tasks.

5.2 User Registration

When an employee leaves the company, their access to computer systems and data must be suspended at the close of business on the employee's last working day. It is the responsibility of the employee's direct supervisor to request the suspension of the access rights.

5.3 User Responsibilities

It is a user's responsibility to prevent their userID and password being used to gain unauthorised access to Harmony systems by:

- Following Harmony's Password Policies
- Ensuring that any PC they are using that is left unattended is locked or logged out.
- Leaving nothing on display that may contain access information such as login names and passwords.
- Informing IT Department of any changes to their role and access requirements.

5.4 Network Access Control

The use of non-Harmony owned PC's connected to the company's network can seriously compromise the security of the network. The normal operation of the network must not be interfered with. Specific approval must be obtained from the IT Department before connecting any equipment to the Company's network.

5.5 User Authentication for External Connections

Where remote access to the Harmony network is required, an application must be made via the IT Department. Remote access to the network must be secured by two factor authentication consisting of a username and one other component.

5.6 Supplier's Remote Access to the Company Network

Partner agencies or 3rd party suppliers must not be given details of how to access the company's network without permission from the IT Department. Any changes to supplier's connections must be immediately sent to the IT Department so that access can be updated or ceased. All permissions and access methods must be controlled by the IT Department.

Partners or 3rd party suppliers must contact the IT Department before connecting to the Harmony network and a log of activity must be maintained. Remote access software must be disabled when not in use.

5.7 Operating System Access Control

Access to operating systems is controlled by a secure login process. The access control defined in the User Access Management section (section 5.1) above must be applied. The login procedure must also be protected by:

- Not displaying any previous login information e.g. username.
- Limiting the number of unsuccessful attempts and locking the account if exceeded.
- The password characters being hidden by symbols.

All access to operating systems is via a unique login id that will be audited and can be traced back to each individual user. The login id must not give any indication of the level of access that it provides to the system (e.g. administration rights).

System administrators must have individual administrator accounts that will be logged and audited. The administrator account must not be used by individuals for normal day to day activities.

5.8 Application and Information Access

Access within software applications must be restricted using the security features built into the individual product. The IT Department of the software application is responsible for granting access to the information within the system. The access must:

- Be compliant with the User Access Management section (section 5.1) above.
- Be separated into clearly defined roles.
- Give the appropriate level of access required for the role of the user.
- Be unable to be overridden (with the admin settings removed or hidden from the user).
- Be free from alteration by rights inherited from the operating system that could allow unauthorised higher levels of access.
- Be logged and auditable.

6 Policy Compliance

If any user is found to have breached this policy, they may be subject to Harmony's disciplinary procedure.

If you do not understand the implications of this policy or how it may apply to you, seek advice from the IT Department.

7 Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by System Administrator.

8 References

The following Harmony policy documents are directly relevant to this policy, and are referenced within this document:

- Remote Working Policy.

The following Harmony policy documents are indirectly relevant to this policy:

- Governance Policy
- Physical Access Policy
- User/Pass Policy
- Incident Policy

9 Key Messages

- User access rights must be reviewed at regular intervals.
- It is a user's responsibility to prevent their userID and password being used to gain unauthorised access to Harmony systems.
- Partner agencies or 3rd party suppliers must not be given details of how to access the Company's network without permission from the IT Department.
- Partners or 3rd party suppliers must contact the IT Department before connecting to the Harmony network.