MATCHWARE
Software for Creative Minds

Data Security Policy

Document Revision: 1.02

MatchWare Inc.
311 S. Brevard Ave
Tampa, FL 33606
United States

T: 1-800-880-2810
F: 1-800-880-2910
usa@matchware.com

MatchWare Ltd
9-11 The Quadrant
Richmond, TW9 1BP
United Kingdom

T: +44 (0)20 8940 9700
F: +44 (0)20 8332 2170
london@matchware.com

MatchWare Germany
Beim Strohhause 31
20097 Hamburg
Deutschland

T: +49 (0) 40 543764
F: +49 (0) 40 543789
hamburg@matchware.com

MatchWare A/S
P. Hiort-Lorenzens Vej 2A
8000 Aarhus C
Denmark

T: +45 87 303500
F: +45 87 303501
aarhus@matchware.com

MATCHWARE
Software for Creative Minds

1 Introduction

The purpose of this policy is to outline essential roles and responsibilities within MatchWare for creating and maintaining an environment that safeguards data from threats to personal, professional and business interests and to establish a comprehensive data security program in compliance with applicable law. MatchWare will use its best efforts to comply with both the law and best practice regarding data security and privacy.

This is done by:

- Respecting individuals' rights
- Being open and honest with individuals whose data is held
- Providing training and support for staff who handle personal data, so that they can act confidently and consistently
- Using best practice and up to date security systems

MatchWare recognizes that its first priority regarding data security and privacy is to avoid causing harm to individuals. Predominantly this means keeping information securely, on a need to know basis, and in the right hands.
This is the top-level policy and, as well as outlining the company's information security objectives and how to meet them, it also includes a requirement for all security related documents to be reviewed periodically to ensure conformity and applicability.
It is the responsibility of all employees to comply with the requirements of this and all policies. Every employee needs to understand his or her obligation to protect company data.

2 Definitions

Data Security Committee. A board of 3 internal people are assigned to be responsible for risk assessment. This committee will meet quarterly to discuss the current risks, enhancements needed and actions that must be taken.
Data Protection Officer. A data protection officer (DPO) is a position within a corporation that acts as an independent advocate for the proper care and use of customer's information.

3 Objectives

MatchWare will:

- Deliver secure, reliable cloud services, on premise and desktop applications for users and other interested parties who need confidence and assurance that the platform is fit for their purpose of sharing and working with sensitive information
- Provide a digital paperless Information Security Management System (ISMS) for staff, integrated into their day-to-day work practices
- Implement a system to identify and assess information security risks and manage a risk treatment plan
- Mitigate the risk of unauthorized or accidental disclosure of confidential information by staff or external parties
- Ensure the integrity and availability of the company's information assets at all times
- Minimize the impact of any security incidents

- Continually improve the company's ability to assess, detect, reduce, avoid and ameliorate information security risks and/or incidents
- Work to avoid a negative impact to MatchWare's reputation and brand
- Protect the information of all interested parties including the personal information of its customers
- Comply with any legal, regulatory or contractual requirements in respect of the data it holds about individuals
- Follow best practice
- Seek to continually improve the company's Information Security Management System

4 Key Risks & Mitigations

The Data Security Committee and an external security consultant have been and will continue to be part of the risk assessment team.

MatchWare has identified the following potential key risks, which this policy, in conjunction with the Risk Treatment Plan, is designed to address:

Risk	Mitigation
Breach of security by an external entity	The development and implementation of Data Security Standards to minimize the risk of data being obtained by hacking or interception. Network security controls and physical perimeter security devices prevent the physical theft of the company's information assets by on-site contractors.
Release of data by a staff member	Staff Awareness Training will be delivered to help staff understand their responsibilities when handling personal data in order to prevent accidental disclosure of sensitive information. Access controls are in place to prevent unauthorized access to the company's information assets. Regular Audits will be conducted to ensure that staff are complying with this policy.
Exposure of sensitive information through hacking of MatchWare products or services	Secure development/coding practices will be employed and development staff training delivered. Testing of our products prior and after release will include, but without being limited to, the OWASP top-ten online vulnerabilities.
Inability to respond to a security breach effectively	MatchWare will develop and manage a Data Security Management system to maximize data security and manage security incidents. A Security Incident Reporting Policy exists outlining steps to be taken subsequent to a security breach.

MATCHWARE
Software for Creative Minds

5 Responsibilities

5.1 Data Security Committee

The role and responsibilities of this committee will be to provide:

- Analysis & Design - The committee is responsible for the analysis and design of the ISMS to ensure that a meaningful security policy as well as effective security solutions exist.
- Administration - To look after the day-to-day administration of access rights, passwords, etc.
- Monitoring - To continuously monitor the security status of the organization, and manage incident response procedures.
- Awareness communication - To ensure awareness communication is conveyed throughout the company to ensure ongoing security awareness and to provide the necessary training programs.

5.2 Data Protection Officer

The Data Protection Officer will have the following responsibilities:

- Dealing with both the day-to-day management of the security team as well as the continuous communication of the importance and value of security measures
- Briefing the Security Committee on Data Protection responsibilities
- Reviewing Data Protection and related policies
- Advising other staff on Data Protection issues
- Ensuring that Data Protection induction and training takes place
- Approving unusual or controversial disclosures of personal data
- Approving contracts with Data Processors

5.3 Specific Other Staff

5.3.1 IT & Network Administrator

- Maintaining a secure network
- Maintaining access control lists to core services
- Implement and run the Business Continuity Plan and Disaster Recovery Plan

5.3.2 CRM and Customer Data Manager

- Manage and control access to Customer Data in the company CRM System
- Ensure that the customer data in the CRM System is stored in compliance with the Data Security Standards

5.3.3 Accounting System Manager

- Manage and control access to Customer Data in the Accounting system
- Ensure that the customer data in the Accounting system is stored in compliance with the Data Security Standards

5.4 Staff

All staff are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work.

5.5 Enforcement
Significant breaches of this policy will be handled under MatchWare's disciplinary procedures.

6 Confidentiality
Because confidentiality applies to a much wider range of information than Data Protection, MatchWare has a separate Privacy Policy.

6.1 Scope
This Policy applies to all employees and third-party agents of MatchWare as well as any other Company affiliate who is authorized to access customer Data. Third-party agents of MatchWare will be required to have a Data Security Policy at least as stringent as this policy.
Third-party agents will also be contractually required, where possible, to return or destroy information assets belonging to MatchWare upon termination of a contract with a third party. This will apply to both virtual and physical information assets.

MatchWare will comply with requests under the Regulation of Investigatory Powers Act 2000 (RIPA) from UK authorities and under the USA Patriots Act from US authorities and Freedom of Information and Protection of Privacy Act (FOIPPA) (British Columbia) if requested to do so.

6.2 MatchWare's Use of Customer Data
MatchWare has a Privacy Policy for Users, setting out how their information will be used.

6.3 MatchWare Staff Responsibilities
All MatchWare Staff are required to sign a short statement indicating that they have been made aware of their confidentiality responsibilities. (See Appendix A)

7 Data Security Standards
All data that that is stored by MatchWare is classified as one of the following data types:

- Public Information
- Company Intellectual Property
- Customer/Personal Information

All data that is classified as Customer/Personal Information must be stored in compliance with the following standards.

All data must conform to the following:

- Be encrypted at Rest
- Be encrypted in Transit using SSL Encryption
- All access to the information must be logged
- Access must be protected by two factor authentication
- All data must be stored in an ISO 27001 or equally secure facility
- All data must be backed up regularly and securely
- All data should be recorded in the Data Security Management System
- Any relevant data security contracts that have been entered into between MatchWare and a Customer must be recorded in the Data Security Management System

- Physical Media Transfer: no customer or private data will be transported using physical media

MatchWare must operate a Business Continuity Plan to deliver continuity of service in the event of a disaster. This plan should cover situations such as:

- Fire
- Flash flood
- Pandemic
- Power Outage
- Theft

8 Staff Training & Acceptance of Responsibilities

All staff who have access to any kind of personal data will have their responsibilities outlined during their onboarding procedures. All staff are required to sign an electronic form signifying that they have read, understood and accepted this policy.

MatchWare will provide opportunities for staff to explore Data Protection issues through training, team meetings, and supervisions.

8.1 Specific Focus Training for Key Handling Roles

8.1.1 Software Developers

Software Developers at MatchWare will be trained to ensure that the architecture of any system that stores personal data is in compliance with the Data Security Standards above.

Prior to release the software will be tested to ensure that it is in compliance.

All Product Owners, Scrum-masters or Project Leaders should ensure that an Information Security Risk Assessment is carried out for each sprint, and when needed, a risk treatment plan is created and followed.

8.1.2 Marketing Staff

Marketing Staff who have access to personal customer information will receive specific training regarding the secure transit and storage of personal data for the purposes of outbound marketing.

9 Policy Review

9.1 Responsibility

The Data Protection Officer will be responsible for reviewing this policy. Audits of all processes within the company will take into account this Data Security Policy at all times.

9.2 Data Security Incidents

Data security incidents will be classified according to severity. Incidents such as unsuccessful exploit attempts that do not involve data loss will be classified as Level 1 - Non Critical Incidents. Level 1 incidents should not trigger a customer notification since there has been no impact to privacy.

Incidents that do involve data loss will be classified as Level 2 - Critical Incidents and should trigger a notification to all customers that are impacted by the data loss.

9.3 Security Breach Response

All MatchWare employees must report any known Security Breach or any incident that is likely to cause a Security Breach. These incidents include thefts of computer devices, viruses, worms, or computer "attacks" that may lead to unauthorized access to confidential information.

10 Appendix A: Confidentiality Statement for Staff

When working for MatchWare, the employee will often need to have access to confidential information which may include, for example:

- Personal information about individuals who are customers or users of MatchWare software
- Information about the internal business of MatchWare
- Personal information about colleagues working for MatchWare

MatchWare is committed to keeping this information confidential, in order to protect people and MatchWare. 'Confidential' means that all access to information must be on a need-to-know and properly authorized basis. The employee must use only the information which has been authorized, and for purposes that have been authorized. The employee should also be aware that under the Data Protection Act, unauthorized access to data about individuals is a criminal offence.

The employee must assume that information is confidential unless you know that it is intended by MatchWare to be made public. Passing information between staff members in our international office, or between MatchWare and a third-party marketing partner who is in compliance with our policy, or vice-versa does not count as making it public, but passing information to another organization does.

10.1 Personnel Security

Upon acceptance of employment at MatchWare, all employees are required to execute a confidentiality agreement and must acknowledge and comply with policies in MatchWare. MatchWare may also conduct criminal record checks depending on the job role.

Access rights and levels are based on the employee's job function and role, using the concepts of least-privilege and need-to-know to match access privileges to defined responsibilities. MatchWare employees are only granted a limited set of default permissions to access company resources, such as their email, and the internal portal of MatchWare.

Terminated employees must return all records containing personal data, in any form, in their possession at the time of termination. This includes all data stored on any portable device and any device owned directly by the terminated employee. If an employee leaves MatchWare, their user ID is disabled and their access to the entire MatchWare corporation is removed.

You must also be particularly careful not to disclose confidential information to unauthorized people or cause a breach of security. In particular you must:

- not compromise or seek to evade security measures (including computer passwords);

- be particularly careful when sending information between our international offices;
- not discuss confidential information, either with colleagues or people outside MatchWare;
- not disclose information — especially over the telephone — unless you are sure that you know who you are disclosing it to, and that they are authorized to have it.

If you are in doubt about whether to disclose information or not, do not guess. Withhold the information while you check with an appropriate person whether the disclosure is appropriate.

Your confidentiality obligations continue to apply indefinitely after you have stopped working for MatchWare.

MatchWare Inc.
311 S. Brevard Ave
Tampa, FL 33606
United States

T: 1-800-880-2810
F: 1-800-880-2910
usa@matchware.com

MatchWare Ltd
9-11 The Quadrant
Richmond, TW9 1BP
United Kingdom

T: +44 (0)20 8940 9700
F: +44 (0)20 8332 2170
london@matchware.com

MatchWare Germany
Beim Strohhause 31
20097 Hamburg
Deutschland

T: +49 (0) 40 543764
F: +49 (0) 40 543789
hamburg@matchware.com

MatchWare A/S
P. Hiort-Lorenzens Vej 2A
8000 Aarhus C
Denmark

T: +45 87 303500
F: +45 87 303501
aarhus@matchware.com