Information Security Policy

Date: April 2018

Chapter 1: Introduction

The confidentiality, integrity and availability of information, in all its forms, are critical to the on-going functioning and good governance of Metaregistrar BV. Failure to adequately secure information increases the risk of financial and reputational losses from which it may be difficult for Metaregistrar BV to recover.
This information security policy outlines Metaregistrar BV's approach to information security. It provides the guiding principles and responsibilities necessary to safeguard the security of the company's information systems. Metaregistrar BV is committed to a robust implementation of Information Security. It aims to ensure the appropriate confidentiality, integrity and availability of its data. The principles defined in this policy will be applied to all of the physical and electronic information assets for which the Metaregistrar BV is responsible.

Chapter 2: Objectives

The objectives of this policy are to:

1. Provide a framework for establishing suitable levels of information security for all Metaregistrar BV information systems (including but not limited to all cloud environments commissioned or run by Metaregistrar BV, computers, storage, mobile devices, networking equipment, software and data) and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems
2. Make certain that users are aware of and comply with all current and relevant Dutch and EU legislation.
3. Provide the principles by which safe and secure information systems can be established for Metaregistrar personnel.
4. Ensure that all personnel understand their own responsibilities for protecting the confidentiality and integrity of the data that they handle.
5. Protect Metaregistrar BV from liability or damage through the misuse of its IT facilities.
6. Maintain confidential information provided by suppliers at a level of security commensurate with its classification, including upholding any legal and contractual requirements around information security.
7. Respond to changes in the context of the organisation as appropriate, initiating a cycle of continuous improvement

Chapter 3: Scope

This policy is applicable to, and will be communicated to all Metaregistrar personnel and upon request to Metaregistrar customers and all information systems used for data storage.
This includes, but is not limited to: Cloud systems developed or commissioned by Metaregistrar BV, any systems or data attached to the Metaregistrar BV data networks, systems managed by Metaregistrar BV, mobile devices used to connect to Metaregistrar BV networks or hold Metaregistrar BV data, data over which Metaregistrar BV holds the intellectual property rights, data over which Metaregistrar BV is the data controller or data processor, electronic communications sent from Metaregistrar BV.

Chapter 4: Policy

4.1 Information security principles

The following information security principles provide overarching governance for the security and management of information at Metaregistrar BV.

1. Information should be classified according to an appropriate level of confidentiality, integrity and availability (see Section 2.3. Information Classification) and in accordance with relevant legislative, regulatory and contractual requirements (see Section 2.2. Legal and Regulatory Obligations).
2. Personnel with particular responsibilities for information must ensure the classification of that information; must handle that information in accordance with its classification level; and must abide by any contractual requirements, policies, procedures or systems for meeting those responsibilities.
3. All users covered by the scope of this policy must handle information appropriately and in accordance with its classification level.
4. Information should be both secure and available to those with a legitimate need for access in accordance with its classification level. On this basis, access to information will be on the basis of least privilege and need to know.
5. Information will be protected against unauthorized access and processing in accordance with its classification level.
6. Breaches of this policy must be reported (see Sections 2.4. Compliance and 2.5. Incident Handling).
7. Information security provision and the policies that guide it will be regularly reviewed, including through the use of annual internal audits.
8. Any explicit Information Security Management Systems run within the company will be appraised and adjusted through the principles of continuous improvement.

4.2 Legal and Regulatory Obligations

Metaregistrar BV has a responsibility to abide by and adhere to all current Dutch and EU legislation as well as a variety of regulatory and contractual requirements.

4.3 Information Classification

The following table provides a summary of the information classification levels that have been adopted by Metaregistrar BV and which underpin the principles of information security defined in this policy. These classification levels explicitly incorporate the General Data Protection Regulation's definitions of Personal Data and Special Categories of Personal Data.

Security Level	Definition	Examples
Confidential	Accessible by personnel with a confidentiality status	Information supplied by suppliers that is covered by a Non-disclosure agreement Information about mergers or acquisitions that are in a planning phase
Restricted	Accessible by certain members of Metaregistrar staff	GDPR-defined personal data (information that can identify an individual) Restricted meeting minutes or reports.
Internal Use	Accessible by Metaregistrar personnel or suppliers on a need-to-know basis	Internal correspondence, meeting minutes, internal memo's or company directives
Public	Accessible by anyone,	Information published on the

	inside or outside the company	Metaregistrar website. Information that can also be found via other sources

4.4. Suppliers

All Metaregistrar BV's suppliers will abide by Metaregistrar's Information Security Policy, or otherwise be able to demonstrate corporate security policies providing equivalent assurance. This includes:

- when accessing or processing Metaregistrar BV assets, whether on site or remotely
- when subcontracting to other suppliers.

4.5 Compliance, Policy Awareness and Disciplinary Procedures

Any security breach of Metaregistrar BV's information systems could lead to the possible loss of confidentiality, integrity and availability of personal or other confidential data stored on these information systems. The loss or breach of confidentiality of personal data is an infringement of the General Data Protection Regulation, and may result in criminal or civil action against Metaregistrar BV. The loss or breach of confidentiality of contractually assured information may result in the loss of business, financial penalties or criminal or civil action against Metaregistrar BV. Therefore it is crucial that all users of the Company's information systems adhere to the Information Security Policy and its supporting policies. All current personnel and other authorised users will be informed of the existence of this policy and the availability of supporting policies, codes of practice and guidelines. Any security breach will be handled in accordance with all relevant company policies, including the Conditions of Use of IT Facilities at the Metaregistrar BV and the appropriate disciplinary policies.

4.6 Incident Handling

If a member of the personnel is aware of an information security incident then they must report it to the Data Protection Officer. Outsiders can also make reports under the Responsible Disclosure rules as published on the Metaregistrar website.

Reported incidents will be handled by the Data Protection Officer and reported back to the incident reporter in question. When customer data is affected, the incident will be reported to the customers involved and immediate measures will be taken to prevent further breach or data leak.

4.7 Review and Development

This policy, and its subsidiaries, shall be reviewed and amended on a yearly basis by the Data Protection Officer and updated regularly to ensure that they remain appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations. Additional regulations may be created to cover specific areas.

4.8 Responsible Disclosure rules

At Metaregistrar, we consider the security of our systems a top priority. But no matter how much effort we put into system security, there can still be vulnerabilities present.
If you discover a vulnerability, we would like to know about it so we can take steps to address it as quickly as possible. We would like to ask you to help us better protect our clients and our systems. Please do the following:

- E-mail your findings to cert@metaregistrar.com. Encrypt your findings using our PGP key to prevent this critical information from falling into the wrong hands,
- Do not take advantage of the vulnerability or problem you have discovered, for example by downloading more data than necessary to demonstrate the vulnerability or deleting or modifying other people's data,
- Do not reveal the problem to others until it has been resolved,

- Do not use attacks on physical security, social engineering, distributed denial of service, spam or applications of third parties, and
- Do provide sufficient information to reproduce the problem, so we will be able to resolve it as quickly as possible. Usually, the IP address or the URL of the affected system and a description of the vulnerability will be sufficient, but complex vulnerabilities may require further explanation.

What we promise:

- We will respond to your report within 3 business days with our evaluation of the report and an expected resolution date,
- If you have followed the instructions above, we will not take any legal action against you in regard to the report,
- We will handle your report with strict confidentiality, and not pass on your personal details to third parties without your permission,
- We will keep you informed of the progress towards resolving the problem,
- In the public information concerning the problem reported, we will give your name as the discoverer of the problem (unless you desire otherwise), and
- As a token of our gratitude for your assistance, we offer a reward for every report of a security problem that was not yet known to us. The amount of the reward will be determined based on the severity of the leak and the quality of the report. The minimum reward will be a €50 gift certificate.

We strive to resolve all problems as quickly as possible, and we would like to play an active role in the ultimate publication on the problem after it is resolved.