Document Reference: SECPOL-0.0.1.GIT
Date: August 5, 2026

Considerations

- wdms.dev values the proper security of its (electronic) systems in which personal data is stored and processed.
- It can nevertheless never be completely prevented that a security incident will occur.
- wdms.dev wishes to meet its legal obligations under the GDPR and other applicable laws.
- wdms.dev has therefore formulated a policy to act as adequately as possible in the event of a security incident.

1 Introduction

This security policy helps wdms.dev:

1. Reduce the risk of IT problems.
2. Plan for problems and deal with them when they occur.
3. Keep operating if something does go wrong.
4. Protect company, client and employee data.
5. Keep valuable company information, such as plans and designs, confidential.
6. Meet legal obligations under the GDPR and other applicable laws.
7. Meet professional obligations towards clients and customers.

IT security problems can be expensive and time-consuming to resolve. Prevention is much better than cure.

2 Responsibility

The person responsible for all security-related issues within wdms.dev, inside and outside of office hours, is reachable via hello@wdms.dev or +297 5939398.

3 Review

1. This security policy is evaluated every year.
2. All clients may request a security audit. The costs will be billed to the client.

4 Baseline security

4.1 Devices

1. All devices use full disk encryption.
2. If full disk encryption is not possible, partial disk encryption is permitted but not encouraged.
3. Devices receive regular security updates.

4.2 Password policy

1. All passwords used have a minimum length of 16 characters. A 32 character password is preferred.
2. Passwords are stored in a password manager.
3. Passwords are not shared via unencrypted means.

4.3 Data storage and retrieval

1. Data shall not be retained longer than required for the duration of the task, or longer than is lawfully required. Lawful requirements take precedence over the duration of the task unless otherwise agreed with the client.
2. Data of third parties (clients) is not retrieved unless there is written confirmation of such a request.
3. Data breaches shall be reported to the relevant governmental agencies.
4. Data stored on unencrypted devices is stored using PGP encryption.
5. Sensitive data is never stored on Google Drive, Dropbox or similar services unless there is an agreement with the client. This is strongly discouraged.
6. Data transfer is always done via encrypted communications, or if the communication protocol does not support encryption, via PGP encryption.

wdms.dev may operate outside of the EEA and may require data from within the EEA.

1. EEA data breaches shall be reported to the Dutch Autoriteit Persoonsgegevens, as Aruba does not have a similar agency.
2. Clients may request reporting to other European agencies if they see fit.
3. The document "Protocol meldplicht datalekken" details further specifics regarding data breaches.