



RFC 2350

DESCRIPTION OF PIPEDRIVE

Last updated on 7th June 2019. Content may subject to changes.

1. DOCUMENT INFORMATION

1.1 Date of Last Update

This is version 1.0 published 2019-04-02

1.2 Locations where this Document May Be Found

File PDF Download location

2. CONTACT INFORMATION

2.1 Name of the Team

Pipedrive Information Security Team

2.2 Address

Mustamäe tee 3a, Tallinn 10615, Estonia

2.3 Time Zone

- **EET, Eastern European Time**

UTC+2, between last Sunday in October & last Sunday in March

- **EEST, Eastern European Summer Time**

UTC+3, between last Sunday in March & last Sunday in October

2.4 Telephone Number

+372 640 6451

2.5 Facsimile Number

N/A

2.6 Other Telecommunication

Available upon request

2.7 Electronic Mail Address

infosec@pipedrive.com

2.8 Public Keys and Encryption Information

N/A

2.9 Team Members

- **Jesse Wojtkowiak** - Head of Information Security
- Information about other team members is available by request.

2.10 Other Information

General information about Pipedrive can be found here:

- Pipedrive Twitter profile : <https://twitter.com/pipedrive>
- Pipedrive Blog : <https://blog.pipedrive.com>

2.11 Points of Customer Contact

The preferred communication channel is the e-mail address infosec@pipedrive.com

If it's not possible to use e-mail, please call the official phone number indicated in p.2.4.

Pipedrive has one team member on duty 24/7.

3. CHARTER

3.1 Mission Statement

- The main goals for Pipedrive Information Security Team are:
- Provide Application and Infrastructure security
- Deal with IT security incidents
- Promote security culture in the organisation

3.2 Locations where this Document May Be Found

The main areas of responsibility of Pipedrive Information Security team are:

- Compliance
- Coordinating and resolving IT security incidents
- Providing security training for the organisation
- Monitoring and acting upon intrusions to the network, application and infrastructure

3.3 Sponsorship and / or Affiliation

Pipedrive Information Security Team is a part of Pipedrive OÜ engineering department

3.4 Authority

N/A

4. POLICIES

4.1 Types of Incidents and Level of Support

Pipedrive Security Team is authorized to handle all types of cyberattacks that would hamper the integrity of Pipedrive OÜ assets or harm its interests.

4.2 Co-operation, Interaction and Disclosure of Information

Pipedrive OÜ highly considers the paramount importance of operational coordination and information sharing between CERTs, SOC's and similar bodies, and also with other organizations, which may aid to deliver its services or which provide benefits to Pipedrive OÜ.

4.3 Communication and Authentication

Pipedrive Security Team protects sensitive information in accordance with relevant Estonian and European regulations and policies within Estonia and the EU.

5. SERVICES

N/A

6. INCIDENT REPORTING FORMS

In case of an incident please report this to infosec@pipedrive.com

In the report answer the following questions: Where? When? What? How? Who?

7. DISCLAIMERS

While every precaution will be taken in the preparation of information, notifications and alerts, Pipedrive OÜ assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.