Information Security Policy

Version history

Version	Date	Change	Author
0.1	13/10/22	First draft	[redacted]
1.0	09/06/2023	Final version ready for publishing	[redacted]
1.1	05/07/2023	Approved by ARC	[redacted]

Review dates

Date	Reviewed by

Metadata

Doc type	Framework
Covers	Information Security Policy
Clauses/controls	Clause 5.2

Contents

Version history 2

Review dates 2

Introduction 3

Scope 3

Policy 3

Approval 3

Introduction

Red Gate Software Ltd (Redgate) recognises that information is an important business asset of significant value to the company and its customers. The confidentiality, integrity and availability of company information needs to be protected from threats that could disrupt business continuity.

This policy has been written to provide a mechanism to establish procedures to protect against security threats, whether internal or external, deliberate or accidental and to minimise the impact of security incidents.

The BOARD OF DIRECTORS has approved this Information Security Policy.

Scope

This policy applies to both physical security and information security in all its forms. It includes safeguarding data whether it's in printed or written form, stored on computer hard drives or removable media (such as USB drives), transmitted across networks, or shared through conversations or phone calls.

Every manager plays a direct role in implementing this Policy within their respective business areas. They are also responsible for ensuring that their staff members fully understand and follow the principles outlined in the policy.

Each employee carries the responsibility of adhering to this policy as well. In cases where staff members fail to comply with the security policy, disciplinary processes may be applied.

Policy

It is the policy of the company to ensure that:

- Information will be protected against unauthorised access or disclosure.
- Confidentiality of information is assured and the integrity of information is maintained
- All regulatory and legislative requirements regarding Intellectual property rights, data protection and privacy of personal information are met.
- Redgate implements and maintains an Information Security Management System (ISMS) that complies with the requirements of ISO 27001:2022.
- Suitable security objectives for the ISMS that support the Business objectives are identified, progressed and achieved.
- Business Continuity and Disaster Recovery plans will be produced, maintained and tested.
- Staff receive suitable Information Security training.
- All breaches of information security, actual or suspected, are reported and investigated by Redgate's security team.
- Failings of the ISMS will be identified and analysed in a timely manner in an effort to continually improve the performance of the ISMS.
- Opportunities to improve the performance of the ISMS shall be identified, reviewed and actioned where appropriate.

Approval

Signed:	[redacted]	Signed:	[redacted]
Title:		Title:	
Date:		Date:	