Scrive AB Information Security Policy

1 Ownership and version history

Timothy Ellis, CISO at Scrive AB

Date/revision	By Whom	Changelog
2022-11-23/1	Björn Hesthamar	Added section about policy exceptions
2022-11-03/1	Tage Borg	Approved
2022-10-13/1	Timothy Ellis	Add exception section for information transfers and general network security.
2022-10-05/1	Timothy Ellis	Clarify training responsibilities. Allow potential exception for client pen testing of non-prod. Add Kolide to MDM policy.
2021-11-06/1	Timothy Ellis	Update roles, language simplifications.
2020-12-18/1	Tage Borg	Approved
2020-12-16/1	Juris Puce	Additions on network and communication security principles (5.11) in line with data to be protected.
2020-05-08/1	Tage Borg	Approved
2020-04-22/1	Timothy Ellis	Remove references to various standards that are only relevant to suppliers. Add section on supplier management. Update data classification table.
2020-03-09/1	Juris Puce	Update by adding numbering and doing general review. Added management commitment 4.3.3 and 4.3.4
2018-12-05/1	Tage Borg, Timothy Ellis	Updated with access control rules
2016-01-29/1	Timothy Ellis	Initial version

Table of Contents

2 Purpose

1. Security is important to Scrive. Ensuring the security of customer and company data is important as our customers, employees and partners hold us in a position of trust with their confidential data.

2. Upholding our reputation as a company that cares about security and maintaining trust is key to obtaining new customers and preventing churn.

3. Reputational damage through avoidable information security/other incidents involving loss or exposure of client data is a serious concern that we have avoided to date by vigilance.

4. Being able to demonstrate due diligence regarding security to potential customers is vital by providing evidence through policy, procedures, compliance with industry/regulatory standards and auditing/certification.

5. This document defines the security policy for the company and covers various topics relevant to all departments.

3 Scope, Management & Application

1. This policy applies to all employees of Scrive AB, contractors, technical infrastructure, third party services and the physical property of the company.

2. Changes shall be communicated to relevant staff and where applicable and appropriate, third parties under a non-disclosure agreement.

3. Scrive shall review this policy and other relevant policies relating to information security on regular basis, but no less than once every two calendar years.

4. Scrive information security policy objectives are as follows

ID	Objective
OB-01	Ensure that Scrive AB is compliant with any applicable information security and data protection legislation and regulations, ensuring compliance with any contractual requirements regarding information security, data protection, business continuity and supplier management/purchasing requirements
OB-02	Increased prospect & customer confidence by gaining certification with relevant industry standards via independent third-party auditing.
OB-03	No information security incidents involving Scrive customer data
OB-04	Effective and information security aware Scrive employees
OB-05	Achieve Scrive SLA objectives for customer facing apps (99.8% uptime for 24x7 operations, excluding scheduled maintenance)

5. Policy exceptions
The CISO may grant exceptions from the requirements as stated in this policy.

Such exemptions will be logged in the document "List of policy exemptions" that is a part of the ISMS.

The CISO will decide if an exemption will require a separate risk assessment as per the risk assessment procedure.

4 Organisation

4.1 Best Practice

1. Scrive employees should use industry standard best practice frameworks where possible, appropriate, and relevant. For example:

    1.1. ITIL (IT service management)
    1.2. OWASP (Web application security)
    1.3. PRINCE2 (project management)
    1.4. Etc

2. Scrive shall apply information security best practice in any project related to information assets starting from the requirements definition phase, into development and deployment as well as operations and disposal.

4.2 Information Security Management

1. Scrive shall develop an ISMS aligned with ISO27001 and other practices/standards deemed relevant by Scrive. The ISMS shall be documented, and its usage logged for internal/external auditing purposes.

2. The management and strategy of information security management shall be subject to yearly reviews. The reviews shall include management of risk and updating the assignment of responsibility through a RACI model.

3. Relevant changes to policies and the management of information security shall be communicated to employees as soon as is practical.

4.3 Departmental Responsibility

1. People and performance are responsible for ensuring all employees receive relevant training on general company policies.

2. Line managers (department heads and team leads) are responsible for ensuring their teams receive role specific training on specific policies and procedures.

3. Senior management are responsible for verifying such training has taken place and that policies/regulations are up to date with requirements.

4. Senior management commits to satisfy security objectives and requirements as laid out in the ISMS scope, and this and other relevant policies.

5. Senior management commits to the continual improvement of the ISMS.

4.4 Information classification

Scrive AB classifies its information as follows:

Data Classification	Examples	Applicable Policy:
1. Publicly Available Data	Data on Scrive AB's public websites, e.g., marketing at scrive.com, social media campaigns, API documentation etc.	Information Security Policy (to classify and for availability)
2. Internal Data	Company policy documentation, non-confidential financial and operational data in our file sharing system, internal meeting videos & notes	Scrive Code of Conduct applies, Information Security Policy
3. Protected Data	● All personal data for which Scrive AB is the controller of ● Confidential data that is available only on an internal need-to-know basis ● Source code & other sensitive intellectual property ● Agreements with customers, suppliers and other third parties ● Invoicing data ● Data relating to employees that is not sensitive, salary information, KPIs etc.	Data Protection Policy, Data Retention Policy, Information Security Policy
4. Highly Sensitive Data	● Personal data for which Scrive AB is the processor of and/or all sensitive personal data Scrive AB is the controller or processor of, that is available only if and to the extent necessary, such as: ● Customer data stored in the Scrive e-signing service ● Sensitive data relating to employees such as information regarding sick days, health issues, etc. ● Information relevant to accessing this data	Data Protection Policy and Data Retention Policy, Information Security policy

As a result of this classification schema following access detailed examples can be used to better understand the impact of the asset classification:

Entity	Classification	Access Details
User SaaS accounts & documents	Internal – highly sensitive	Strictly necessary - Limited to trusted IT, support and SRE staff involved in customer support and problem debugging.
Internal policy documentation	Internally available	Internally available - Provided to all employees of Scrive for reference.
Risk Assessments	Internal - confidential	Internal need-to-know - Risk assessment data shall be made available to all employees involved in the risk assessment and treatment process.
External policy documentation	Publicly available	Documentation is either made publicly available or can be made available on request

4.5 Software Development

4.5.1 Source Code Access

1. Source code access to software projects produced by Scrive shall be controlled at minimum with usernames and passwords but ideally using public key authentication and two factor authentication.

2. Access to repositories shall be restricted to only the people who need access to them to carry out development work.

3. A code review policy shall be in place to ensure that only approved code reaches the staging/production branches.

4.5.2 Cryptography

1. Cryptography shall be used to protect sensitive information. It shall be used responsibly so that methods that are considered broken or cryptographically weak are not employed.

2. Should a cryptographic standard in use by the company that was previously regarded as secure be considered broken or weak following technological, cryptographic, or hacking related advancements that standard shall be phased out and replaced.

3. Information such as passwords shall use strong one-way encryption, i.e. hashing. Other information such as user documents shall use a strong reversible encryption algorithm. Should an existing hashing method be classified as weak it may optionally be mitigated by hashing the weak hash with a strong one (hence it is continued to be used in a secure manner) or replacing it altogether.

4.5.3 Other Development Security Issues

Where possible controls shall be put in place to prevent data leakage or compromise between clients using our cloud service.

5 Infrastructure Management

5.1 Wireless Networks

1. Wireless networks shall enforce the strongest encryption standards possible, and not allow easily compromised older standards to support legacy devices. However, such networks should be capable of supporting the majority of devices operated by Scrive.

2. Wireless networks shall not be directly connected to secure networks, such as SaaS product management networks. Employees on such networks should use VPN connectivity for such access.

3. Network hardware deployed in offices should optionally have QoS (*quality of service*) capability for mitigating utilisation issues and preventing abuse. The network perimeter of wireless networks shall be firewalled.

4. Where possible, if manageable in a way that does not interfere with network usage the following controls shall be implemented:

   4.1. Network traffic threat analysis using DPI (*deep packet inspection*)
   4.2. URL scanning to prevent users from accessing hostile web sites.

5.2 Vulnerability & Penetration Testing

1. Network penetration/vulnerability testing shall be carried out at least yearly on all public endpoints for SaaS services operated by Scrive as per our requirements of the relevant sub-sections of ISO 27001 A.13.1.

2. Checks should be carried out periodically in house using open-source vulnerability testing utilities such as OpenVAS. Where possible specialist

security consultants should be periodically employed for more in-depth testing and reporting.

3. In the context of SaaS offerings, application penetration/vulnerability testing shall be carried out as at least yearly on third party software (for example web server & other open-source applications) and *shall* also be carried out at least yearly on software produced internally.

4. The results of network/application penetration/vulnerability testing shall usually not be shared with third parties outside of Scrive. Under certain circumstances that have reasonable justification the most recent results *may* be provided under NDA at the discretion and agreement of the CISO or CTO.

5. Clients of Scrive shall not generally be allowed to carry out network or application vulnerability testing of Scrive systems, as this has serious privacy implications for SaaS users and possible availability implications to our SaaS products. Exceptions may be made for non-production environments not containing customer/user data under very special circumstances at the discretion and agreement of the CISO or CTO.

5.3 Segregation

1. Networks, environments (i.e. development, staging and production, office), services (i.e. web, application, database servers/containers etc) and sensitive systems shall be segregated, including routing controls where possible, from each other using relevant security practices to ensure:

   1.1. Production data is kept separate from non-production data
   1.2. Protection and isolation of sensitive data
   1.3. Compliance with any legal/contractual/regulatory requirements

2. Where management interfaces/diagnostic ports/configuration interfaces are applicable these shall also be segregated onto another network or by using other technical and/or physical controls where possible.

3. Where possible segregation of duties shall be applicable to prevent unauthorised or unintended modification of the information assets of Scrive.

5.4 Hosting and Third-Party Services/Suppliers

1. When purchasing hosting or third-party services/suppliers it shall be ensured they are not geographically located in areas with high risk of environmental disasters such as flooding, hurricanes, tornadoes, earthquakes etc.

2. Scrive requires that as many of the following security measures as possible *should* be implemented at third-party hosting services where our production infrastructure is deployed:

   2.1. 24/7 manned security presence

2.2. CCTV
2.3. Multifactor and/or biometric access to facilities
2.4. Redundant power supplies and UPS
2.5. Automatic fire detection & suppression systems
2.6. Adequate and redundant HVAC systems
2.7. Equipment is sited in a high security facility
2.8. Power/network communication cabling should be tamper-proof

3. The hosting provider where Scrive production systems are located shall follow industry best practices/standards and carry certifications to prove compliance. These standards should include the following or equivalent:

   3.1. ISO/IEC 27001:2013 (where any Scrive Protected or Highly Sensitive Data is processed.
   3.2. PCI/DSS self-assessment (for locations where and when Scrive customers' credit card data is processed)

4. Hosting and third-party services *should* be located within the EU to satisfy legal requirements and rulings with regards to the protection of personal data of citizens of the EU.

5. For services located outside of the EU compliance via "standard contractual clauses" that are acceptable under EU law *shall* be required. These shall be subject to audit via Scrive's legal counsel. Typically, such services rarely pass internal due diligence processes and are strongly discouraged.

6. Third party data processing facilities or services shall be reviewed with the requirements of this and other policies in mind by the person responsible for this aspect of supplier management before being approved or rejected.

7. Services shall be reviewed periodically at least every 5 years after the last complete review for compliance with the policies within this section and additionally reviewed to verify that legal and regulatory requirements are met for the country where the third-party service/hosting company is based.

8. Third party services should be reviewed for uptime/performance/etc and if necessary, replaced. Finally, should changes to IS related agreements to third party service occur these services should be reassessed.

5.5 Access to Scrive Systems & Networks

1. Access to production systems is limited to an authorised set of employees. This includes the DevOps team and a very limited sub-set of employees from other engineering teams for debugging or maintenance purposes only.

2. General access to other systems shall be restricted so that users are only provided with access to systems that they need to carry out their work.

3. Third parties such as external companies, contractors or any other external entities are not allowed access to such systems or networks under any circumstances, other than the publicly provided website or API endpoints.

4. The only exception to the access policies to Scrive systems and networks may be auditors or security/development consultants working with Scrive authorisation under an NDA.

5. Business processes to be implemented by third parties affecting information assets on Scrive systems/networks/data processing facilities shall be risk assessed. If such processes are deemed appropriate controls shall be put in place to manage access.

6. Access to Scrive networks shall be reviewed at least twice yearly. User & administrator rights shall be verified to be correct in a reportable manner.

7. Temporary access to systems and networks *shall* be logged and recorded and periodically reviewed every 90 days, access still existing at this time *should* where necessary be re-authorised.

8. Key management shall be employed to manage cryptographic technology used to access systems from a centralised KMS to save time managing keys on systems, improving response time to support requests and security incidents.

9. Where public endpoints exist that provide access to Scrive networks or services, for example VPNs & web based management interfaces, they shall be protected using two-factor authentication/public key authentication/other security methods where possible.

5.6 Access Control Rules

1. In Scrive eSign, there are three roles: user, company admin, partner admin and Scrive Administrator. These roles have the following rights:

Role	Read	Create	Edit	Delete
User	Own documents, shared templates, own personal information	New documents, templates, shared templates, own API keys	Own documents (non-closed), own templates, own personal information	Own documents, own templates, own API keys
Company admin	All documents, shared templates, own personal information in company, partial personal information for other users in company, company information	New documents, templates, shared templates, user	Own documents (non-closed), own templates, own personal information,	Own documents, own templates, own API keys, documents belonging to

		invitations, own API keys	company information	other users in company
Partner admin	Personal information for users in any child company, Child company information	Companies (that then become child companies), users in child companies	Companies, users in child companies	Nothing
Scrive administrator	Personal information for users in any company, company information, metadata (timestamps, document name, signatory names, document status) for any document	Companies, invitations for users in any company	Companies, users in any company	Companies, users in any company

2. Partner admin is a role than can be held in addition to holding another role.

3. Access to the Scrive Infrastructure is more segmented than access to the actual product. Key roles in place are:

   3.1. Developers (Dev)
   3.2. QA Staff (QA)
   3.3. Service Reliability Engineers (SRE)
   3.4. Deployment Engineers (DE)
   3.5. IT Staff (IT)

4. These roles are mapped to access roles in the service infrastructure, however all roles mentioned above have VPN access.

5. The table below describes the level of access that the various roles have to the different environments Scrive hosts on AWS.

	Dev	QA	SRE	DE	IT
Core Dev	RW	-	-	-	RW
Core API-testbed	-	-	RW	RW	RW
Core Staging	-	-	RW	RW	RW
Core Production	-	-	RW	RW	RW
Go Dev	RW	-	-	-	RW
Go API-testbed	-	-	RW	RW	RW
Go Staging	-	-	RW	RW	RW
Go Production	-	-	RW	RW	RW
Features-testbed	RW	-	-	-	RW
Middlewares	-	-	-	RW	RW
Teamcity	RW	RW	RW	RO	RW
ELK (Centralised Logs)	RO	RO	RO	RO	RO
AWS Console excluding Lambda	-	-	-	-	RW

AWS Console for Lambda	-	-	RW	RW	RW

6. Scrive shall, when the organisation so permits, segregate duties further, by splitting up existing roles into several roles.

7. Using AWS IAM, further restrict access to higher management functions in the AWS console.

8. Use Ansible to restrict IT system level access to certain items, for example RW access to centralised and local logging facilities, limiting access to certain systems or environments etc.

5.7 Documentation

1. Scrive systems and operating procedures should be documented and maintained. The documentation shall be stored in a centrally available location.

2. Scrive policy documentation shall be made available to the company but be secured in such a manner that only authorized management staff are able to edit the company policies.

3. Documentation may be made available to third parties under NDA at the discretion of Scrive to enhance the support/sales/compliance processes.

5.8 Baseline Protection

Scrive shall implement baseline protection measures, at least on all components of its production network and elsewhere as appropriate to protect information assets.

5.9 Malicious Code

1. Controls shall be put in place where possible to prevent malicious code, for example malware, and other unauthorised software from functioning. Such measures shall include intrusion detection systems, anti-virus, and any other applicable controls.

2. Users should receive periodic training on best practice to help avoid information security incidents involving malicious code, particularly on best practice in the use of electronic messaging.

5.10 Mobile device policy

1. All Apple mobile devices shall be configured to be used through Scrive deployed Mobile Device Management (MDM) tooling.

2. All Apple mobile devices shall have MDM configured to enable screen locking immediately after the screensaver is enabled, locking after not using device for specific period and remote wiping for lost devices.

3. All Linux computers *should* have the Kolide compliance software installed. This will become a hard requirement on completion of the Kolide rollout.

4. All mobile devices with technical capacity for this functionality shall have malware protection enabled.

5. Users are responsible for not keeping Scrive sensitive data locally on mobile devices.

6. Exceptions to usage of non-Apple devices must be approved by CISO and are allowed only in specific scenarios:

    a. Developers needing Linux machines
    b. Video processing due to specific needs
    c. Cases where a justification is deemed sufficient by CISO

5.11 Information transfers and general network security

1. Any transfer of protected and highly sensitive data can be done only through secure means of communication and by using securely encrypted means of communication;

2. Any Highly sensitive data at rest should be encrypted (either file system, database, or other sufficient level);

3. Transfer of highly sensitive data is only permitted with specific logged approval of Scrive CISO and using only approved method

4. Any changes to network controls or configuration which might affect access to Protected data or highly sensitive data must be evaluated from a risk perspective

5. Any encryption key used to encrypt information during transmission should either use Public/Private key type of encryption or in case of symmetric encryption the key should be passed on to other party securely, using another means of communication

6. NTP shall be configured on servers and/or containers as necessary to support evidence of time in logs and customer processes.

5.12 Exceptions to information transfers and general network security

1. The Microsoft SQL Server Express database hosted on AWS in the vendors VPC for the purposes of Sharepoint integration of SaaS products shall be exempt

from the disk encryption requirement due to its operation otherwise being prohibitively expensive.

6 Scrive Assets

6.1 Facilities

1. Scrive managed facilities have various security requirements including:

    1.1. That ingress/egress points to the facilities include an acceptable security perimeter including measures such as passcode entry in combination with keys and alarm systems
    1.2. That equipment within such facilities is sited securely and in a manner that it cannot be tampered with by unauthorized users
    1.3. That network/telecommunications/power cabling is tamper proof

6.2 Inventory/Asset List

Scrive information assets shall be entered into an inventory that is maintained with a list of owners of each asset.

7 Supplier management

1. Scrive should make this and other relevant policies available to suppliers and require them to follow these policies as part of agreements where possible

2. In case any parts of Scrive ISMS are provided by suppliers or suppliers have access to any relevant information protected by ISMS, Scrive shall define supplier liabilities, what controls the supplier is expected to implement and enforce them within contracts (e.g. requirements for suppliers to have ISMS with the scope relevant to services provided)

3. Scrive shall retain information and be informed by suppliers about any 3rd party involved in supply chain who might as part of service provisioning or delivery process gain access to Scrive information deemed “Protected data” or “Highly Sensitive Data”