SAFEQ Cloud®

SECURITY WHITEPAPER

Content

Y SOFT Security Overview ..... - 3 -

The Shared Security Responsibilities ..... - 10 -

Y SOFT Product Infrastructure ..... - 12 -

Application Protection ..... - 15 -

Customer Data Protection ..... - 19 -

Data Backup and Disaster Recovery ..... - 20 -

Identity and Access Control ..... - 21 -

Organisational and Corporate Security ..... - 23 -

Incident Management ..... - 25 -

Compliance ..... - 26 -

Y SOFT Security Overview

DOCUMENT SCOPE AND USE

This document provides an overview of the security features and practices implemented in YSoft SAFEQ Cloud solution. Information contained in this document is intended to assist Y Soft partners and end customers in understanding how the security of the solution is ensured and how the end customers may leverage the security features of the solution to maintain the confidentiality, integrity, and availability of their data.

The target audience for this document includes IT professionals, security professionals, and decision-makers responsible for selecting and implementing print management solutions in their organizations. This document also provides insight into the security controls implemented by Y Soft to ensure compliance with relevant regulations and standards.

All information in this document is based on the current state of technology and the best practices implemented by Y Soft. The content of this document is subject to change as new threats may emerge and new security controls are implemented.

This document does not replace or supersede any contractual agreements, terms of service, or service level agreements between Y Soft and its partners and customers. It serves as a supplement to these documents to provide additional information and transparency into the security practices implemented by Y Soft in relation to YSoft SAFEQ Cloud.

OUR COMPANY AND PRODUCTS

Y Soft Corporation is a multinational software and electronic hardware company founded in 2000, which operates in 21 countries. Since 2000, Y Soft has been on a mission to simplify and automate everyday work by clearing the path for businesses to focus on what matters. Today, more than 29,700 customers, including 44% of the Global Fortune 500 companies, enjoy Y Soft products.

YSoft SAFEQ Cloud is an all-in-one print infrastructure solution designed for organisations that want to unburden themselves from running a complex IT print infrastructure while gaining all the benefits of a Software as a Service (SaaS) solution.

YSoft SAFEQ Cloud enables organisations to take advantage of centralised cloud services, reduce and even eliminate the need for decentralised and costly server and network infrastructure. The solution provides many of the basic features of a standard print management solution in one user-friendly software solution and integrates easily with most of the market leading MFD (multifunction devices) print vendors. This makes YSoft SAFEQ Cloud the ideal platform for organisations of any size that wants to reduce infrastructure complexity, user support and centralize print operation without having to think about the choice of print vendors.

Utilizing a multitenant architecture and unique technologies to offer single driver and file compression, YSoft SAFEQ Cloud can enable organisations to optimise administrations and user experience by only being exposed to one print driver and still print and release on any MFD device across the organisation.

YSoft SAFEQ Cloud is designed to offer several hosting options depending on which business model is being used. It can accommodate businesses with:

- Their own datacentre
- No datacentre
- On-premises private cloud solution, for customers with high security requirements

Y SOFT INFORMATION SECURITY STATEMENT

Y Soft Corporation is committed to protecting its information assets from all threats whether internal or external, deliberate, or accidental. This is to ensure the preservation of Confidentiality, Integrity, and Availability (C.I.A.) of information that guarantees business continuity, minimizes business loss by detecting and preventing security incidences.

The starting point of the Information Security Policy is to ensure the uninterrupted fulfillment of Y Soft Corporation's strategic and economic goals, including the protection of information assets and the interests of our customers, business partners, and all relevant stakeholders. The fulfillment of the Policy is achieved by the implemented Information Security Management System (ISMS) and is based on personal commitment, responsibility, and activity, not only for management, but also all employees of the company.

The main goal of this ISMS is to adequately ensure the availability, integrity, and confidentiality of information in all activities related to the company's business with an emphasis on the provision of our cloud services. An integral part is the Management of Compliance with regulatory and legislative requirements.

Security in the company is managed by the Chief Information Officer. Security roles are established to ensure the performance of security functions in the company. Roles are performed by company employees or provided by the services of external entities.

The Management of Y Soft shall review this policy at regular intervals for continual suitability.

The Risk Management process is an essential tool for damage prevention. Risks are analyzed and prioritized based on their severity in connection with possible impacts, the importance of secured activities and the company's ability to release the necessary resources.

The Management System is subject to continuous monitoring, evaluation of the state of safety and implementation of adequate corrective measures.

Security awareness is constantly being strengthened in society. The qualifications of the staff responsible for performing the safety roles are systematically cultivated and controlled by the management.

Y SOFT SECURITY AND RISK FOCUS

Y Soft's primary security focus is to safeguard our customers' data. This is the reason that Y Soft has invested in the appropriate resources and controls to protect and service our customers. This investment includes the implementation of a dedicated Security and Product Security team. This team is responsible for Y Soft's comprehensive security program and the governance process. We are focused on defining new and refining existing controls, implementing, and managing

the Y Soft security framework as well as providing a support structure to facilitate effective risk management. Our Chief Security Officer oversees the implementation of security safeguards across Y Soft and its products.

SECURE BY DESIGN FOR BOTH CLOUD AND EDGE COMPUTING

YSoft SAFEQ Cloud service delivers cloud-based print, copy and scan services with optional edge components as per customer needs.

By utilizing optional Edge virtual appliances or physical devices, we stand by our commitment to privacy even when on-premises infrastructure is required by the customer. Document storage and processing remains local to ensure that document integrity and privacy is maintained. Only the print job's selected metadata travels encrypted to the cloud for management and reporting purposes. Document content remains secure because it never leaves your premises and thus never reaches cloud components. Data which is not present in cloud cannot be externally compromised, because they simply are not "there."

Customers may choose to implement YSoft SAFEQ Cloud in either shared or reserved instances. With reserved, the document processing and storage is dedicated to one customer, so data is never exposed to any other entity. Document content and user identity thus also remains secure.

HERE IS HOW IT WORKS

YSoft SAFEQ Cloud (software) is embedded on multifunction devices (MFDs) and printers at the business location. There, it is either connected with a Y Soft Edge device, (hardware or virtual appliance) or directly to a cloud instance. The edge device is responsible for processing jobs onsite. Though it does the work of a server, the Edge device, much like a network router, is self-contained and needs no customer maintenance. It simply sits there doing what it needs to do—processing print jobs. A Virtual Appliance operates in a comparable manner to the Edge hardware device but is run on a customer-supplied server or virtual machine.

	Zero Trust Infrastructure	YSoft SAFEQ Cloud uses software-defined infrastructures in Cloud and Edge to provide auto-scaling and advanced networking and security. In Y Soft view of Zero Trust approach, there are no trusted networks and zero implicit trust among services, instances, and clients. All system services, components, Edge devices and (optionally) deployed MFDs are mutually authenticated, and all communication is secured using industry-standard protocols, such as TLS (Transport Layer Security) 1.3. Zero Trust is often perceived as a network level architectural decision. Yet we believe that the Zero Trust approach needs to be applied holistically. Y Soft SAFEQ Cloud service provides "beyond the network" Zero Trust capabilities, such as individual service recycling and tenant infrastructure recycling in multi-tenant environments.

		The following network protocols are primarily used: HTTPS (HTTP over 1.3 with server authentication) HTTPS with mTLS (HTTP over 1.3 with mutual-TLS authentication) IPPS (IPP over HTTPS) mTLS refers to TCP communication secured with mTLS (mTLS 1.3) Communication happens in 3 tiers: **Cloud**: services exposed via publicly accessible endpoints (public cloud) **Edge 2 Cloud**: bi-directional communication from Edge devices to Cloud services **On Premise**: Edge 2 Edge, Mobile Clients, and Desktop Clients
	Zero Trust Secure Edge	In the case of optional Edge components, Zero Trust needs to be applied on Edge devices too. Again, securing “just” services / applications running on the Edge dice is not enough. Y Soft approach to Secure Edge using the Zero Trust principles provides the following capabilities: **Trusted and Secure Device Identity** - Each device provides trusted bond with its associated cloud tenant for management. Such identity is sufficient for establishing trust and unique identification of the device. This identity includes, but is not limited to, secure establishment and storage of encryption and digital signing keys in specialized secure enclave on your device. **Trusted Path** - Y Soft secure Edge devices provide trusted boot and trust path capabilities, which ensure that only trusted operating system can be booted and run on the device. This ensures decreased or zero attack surface and protection of customer privacy and data integrity. **Mutual Service Authentication** - Once secure cloud and edge environments are established, all services and devices (including optional authentication for MFDs – if supported by the MFD vendor) are performed using mTLS industry standard protocol. **Cloud Manageability** - All cloud and especially edge deployments are securely manageable from cloud, including seamless remote deployments and rolling / transitional updates and upgrades. Device 2 Cloud communication is secure, including mutual authentication.

		Remote Wipe of Customer Data - All customer data hosted on Edge devices can be remotely wiped using the cloud management capabilities.
Data transfer	Print Job Data in transit: Workstation to Edge device & Edge device to the multifunction printer.	Because the Edge device is secure in your trusted network, all print job data stays safely within your company's boundaries. Data is transferred via secured IPPS protocol for printers that support higher levels of data security. Support for legacy, unsecured protocols, such as LPR is also available, yet disabled by default.
	Print Job Data in transit: Workstation to Cloud & Cloud to the multifunction printer.	Data is transferred via secured TCP or HTTPS protocol to cloud and downloaded by trusted multifunction printer using device authenticated HTTPS protocol from the cloud in context of user authenticated to the multifunction printer.
	Scan Job Data in transit: Multifunction printer to Edge cloud	Scan data are transferred to the cloud services using device-authenticated (with context of specific user) WebDAV/S protocol.
	Print job metadata: Edge device to cloud	Print job metadata is used for reporting purposes. Reports provide insight and an audit of print services use. Metadata includes print, copy and scan activity on printers or groups of printers, users or groups of users. It does not include the content of a document.
Data Access Permissions & Limitations	RBAC	Access to customer data is limited to authorized Y Soft or Y Soft partner reseller employees who require it for their job and whose data access is logged and only in specific cases. Secure portal communication between an administrator and the management portal using TLS/HTTPS, compatible with the version supported by the client. YSoft SAFEQ Cloud may authenticate a user's identity at the print device by verifying against a company's directory. The device connects to Active Directory using an LDAP (Lightweight Directory Access Protocol) connector on the Edge device synchronized to the cloud service via secured line. The product does not access any user passwords or other private data. For cloud directories (Azure AD (Active Directory), Google, …) standard OAUTH2 protocols are used. For shared infrastructure customers, secured separation between tenants' User Directories are in place.

	SSO	Use of Single Sign-on (SSO) allows you to authenticate users in your own systems without requiring them to enter additional login credentials to use the YSoft SAFEQ Cloud.
	Internet security protocols	Browser access to the management portal is through HTTPS, using role-based access within the application, authenticated via SAML, OAUTH2 and OpenID Connect industry standards.
	Cloud SQL Database (metadata)	Application metadata, configuration, job metadata, reporting and generic user information are stored in cloud provider's managed SQL database. A very limited number of highly trained specialists responsible for application maintenance and management on an as-needed basis have administrator access to the databases. Access to the data is logged to cloud provider's audit logs.
	Application Logs	Application logs for troubleshooting are collected in cloud provider's central log repository and available to support personnel on an as-needed basis. Logs do not expose any access/credentials related or document content information.
	Customer (tenant) specific metadata (users, devices, reporting, print job information, …)	Role-based administrator access allows portal management of devices and system reports. This access can be assigned to the business' administrator and/or maintained by a certified Y Soft partner reseller. Access to the customer application management web interface is limited to support personnel on an as-needed basis upon authorization by the customer during incident management sessions. For (alternative) shared infrastructure deployments, there is also a set of support accounts granted only to an extremely limited number of highly trained specialists responsible for application maintenance and management on an as-needed basis. Access to the data is logged to cloud provider's audit logs.
	Application / Edge Device Updates	Edge device application is managed by industry-standard tools and protocols and systems provided by cloud provider platform. Deployment is managed via tiered environment with separated development, testing, staging and production environment plus dedicated deployment plans per customer. Updates are transferred via encrypted and device authenticated HTTP/S communication. Application components are stored in cloud provider's secured artifact repository and deployed to cloud instances and edge devices using automated and secured state-of-the are tools (also provided by the cloud platform). All artefacts are created and deployed using secured development lifecycle process

		and managed by team of highly trained specialists responsible for application maintenance and management
Shared Infrastructure	Shared Infrastructure	One feature of shared infrastructure that makes it so attractive to businesses is its low cost. This is due, in part, to servers managed by the service provider and the sharing of an underlying cloud-based application. The cloud-based application, in this case YSoft SAFEQ Cloud provides services to multiple businesses, each one considered a separate 'tenant.' In this multitenant scenario, each tenant must have its own metadata identification, separation, and protection All above mentioned points apply Each tenant owns a unique security certificate associated with its metadata

USER IDENTITY MANAGEMENT

YSoft SAFEQ Cloud is built on modern authentication methods (OAuth 2.0) and utilizes Single sign-on (SSO) provided by external Identity Providers such as Microsoft Azure Active Directory. SSO is a session and user authentication service that permits a user to use one set of login credentials to access multiple applications. Customers who want to use YSoft SAFEQ Cloud, we recommend them to use an external Identity Provider that manages the Internet identity of all their users. This approach allows admins to define the required level of user identity protection by enforcing multi-factor authentication. Another advantage is that users log in at browsers which they know (and consider secure) via Microsoft's authentication page, and YSoft SAFEQ Cloud merely receives information on the results. User credentials are safely confirmed by their external Identity Provider and never shared with the service provider (YSoft SAFEQ Cloud). The external Identity Provider provides YSoft SAFEQ Cloud only basic user details such as their first name, last name, and username based on permissions and grants set in the Identity Provider

At MFDs, the users use cards and card readers to authenticate. Upon their first card authentication at the MFD, each user is asked to confirm their identity so that the card may be assigned permanently to their account.

Whenever a user logs in, YSoft SAFEQ Cloud refreshes the user details from the external Identity Provider – role membership changes, name changes and account deactivation/reactivation.

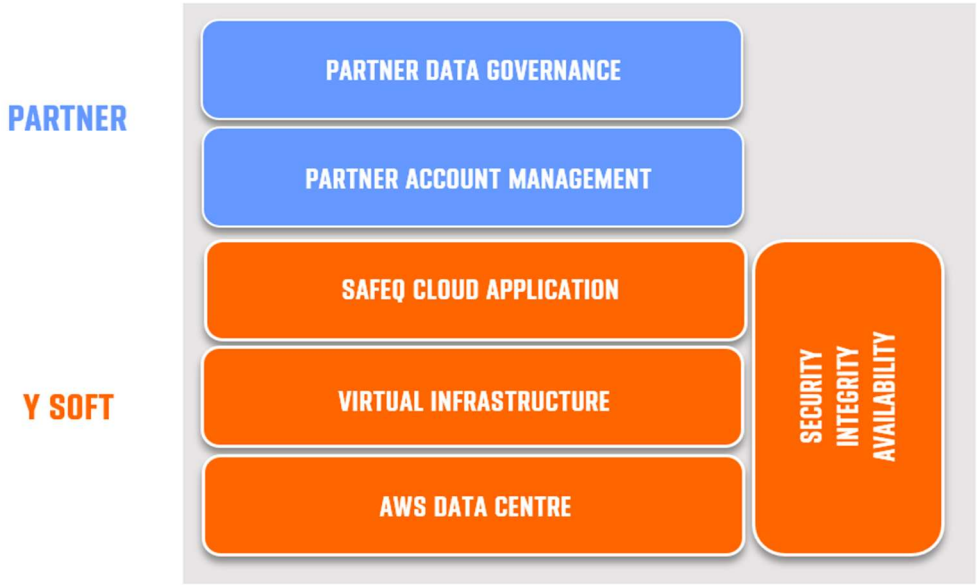
The Shared Security Responsibilities

Y Soft and its Partners are jointly responsible for the security of their customers' print infrastructure. Ysoft SAFEQ Cloud can be hosted either by Y Soft, by a Partner (within a Data Centre selected by Partner) or by the Customer.

HOSTED BY Y SOFT

When Y Soft is responsible for the security of the underlying cloud service platform, network connectivity of the application, and physical data centres, and partners/customers are responsible for the user management, account management and data governance and rights management.

The shared security responsibility model is different than the typical security model a customer would see in an on-premises print environment. By using Y Soft's Cloud infrastructure, customers can leverage the underlying security, integrity & availability that YSoft SAFEQ Cloud provides, attaining a higher level of security relative to the investment required when managing the environment themselves.



SECURITY RESPONSIBILITIES OF YSOFT

In general, Y Soft is responsible for the security of its Virtual infrastructure, OS, and cloud services/products, and provides customers with the technical means necessary to protect their print service

- Y Soft ensures the cloud platform security by:
- Protecting the physical security of cloud data centres by outsourcing this to best in class vendors such as AWS.
- Protecting the security of software, and network of the cloud platform by means of OS- and database-patch management, network access control, Anti-DDoS, and disaster recovery, etc.;
- Identifying and fixing security vulnerabilities of the Application or the Cloud service in a timely manner without affecting partners / customers ' service availability;

- Cooperating with independent third-party security regulation to evaluate security and compliance of Y Soft cloud service security

In Y Soft-hosted solutions, data is hosted by major third parties, who have a contractual obligation with us, ensuring they handle data according to GDPR-requirements.

SECURITY RESPONSIBILITY FOR PARTNERS/CUSTOMERS

Y Soft Partners/Customers (Data Controller) are required to meet strict safety and security demands, and these requirements naturally involve handling documents through YSoft SAFEQ Cloud. We see this as an opportunity and take on a proactive approach to fulfilling our duties, thereby helping you fulfil yours. This section describes individual actions that foster data security during the YSoft SAFEQ Cloud lifecycle:

- Y Soft will never use personal data for any other purposes than delivering the YSoft SAFEQ Cloud service. Further, it is ensured that any present and future sub-suppliers uphold local or regional data protection laws. For example, this means all data is stored on servers within one region, unless otherwise explicitly agreed upon.
- The customer/Partner-appointed administrator may however choose to retain the document in Ysoft SAFEQ Cloud for a predefined number of minutes/hours hereafter – for example to enable re-print. This will not impose a major security risk, other than more data is available in case of a breach.

OUR SECURITY AND RISK MANAGEMENT OBJECTIVES

- We have developed our security framework using best practices in the SaaS industry. Our key objectives include Customer Trust and Protection – consistently deliver superior product and service to our customers while protecting the privacy and confidentiality of their information.
- Availability and Continuity of Service – ensure ongoing availability of the service and data to all authorized individuals and proactively minimize the security risks threatening service continuity.
- Information and Service Integrity – ensure that customer information is never corrupted or altered inappropriately.
- Compliance with Standards – we design our corporate security program around the industry cybersecurity best practice guidelines including the Center for Internet Security (CIS) Critical Security Controls. Our controls governing the availability, confidentiality, and security of customer data are also designed to be SOC 2 compliant.

Y SOFT SECURITY CONTROLS

To protect the data that is entrusted to us, Y Soft utilizes a defense-in-depth approach to implement layers of security controls throughout our organization. The following sections describe a subset of our most frequently asked about controls.

Y SOFT Product Infrastructure

CLOUD INFRASTRUCTURE SECURITY

Y Soft does not host any YSoft SAFEQ Cloud within its corporate offices.

Y Soft outsources hosting of its product infrastructure to leading cloud infrastructure provider, Amazon Web Services (AWS). Our hosting provider guarantees between 99.95% and 100% service availability ensuring redundancy to all power, network, and HVAC services.

Y Soft's AWS product infrastructure resides in the USA, Canada, The European Union, UK, Singapore, and Australia regions. AWS maintains an audited security program, as well as physical, environmental, and infrastructure security protections. Business continuity and disaster recovery plans have been independently validated as part of their SOC 2 Type 2 and ISO 27001 certifications.

Our solution has been setup using 3 different Availability Zones in each of the regions where the solution is deployed. This means that we have multiple servers connected in a cluster environment with failover into different physical locations. If one zone for whatever reason fails, other servers located in a physically different location will automatically take over, completely seamless to users.

Our platform regularly undergoes independent verification of security, privacy, and compliance controls, achieving certifications against global standards to ensure it is the most secure in the industry. Recently our environment was assessed by IBM Nordcloud. Their report "Well-architected review" confirms a high level of operational excellence, security, reliability, and performance efficiency for the YSoft SAFEQ Cloud AWS production environment.

NETWORK SECURITY AND PERIMETER PROTECTION

The Y Soft product infrastructure enforces multiple layers of filtering and inspection of all connections throughout the platform.

Network-level access control lists are implemented to prevent unauthorized network access to our internal product infrastructure. Firewalls are configured to deny network connections that are not explicitly authorized by default, and traffic monitoring is in place for detection of anomalous activity.

Changes to our network security are actively monitored and controlled by standard change control processes. Firewall rulesets are reviewed on an annual basis to help ensure that only necessary connections are configured.

Protecting our Cloud environment in AWS we use several AWS professional tools, including:

- **AWS Security Hub** evaluates configuration items to assess whether the AWS resources comply with the desired configurations defined by the defined security standards.
- **AWS GuardDuty** which is a threat detection service that continuously monitors for malicious activity and unauthorized behaviours to protect the AWS account.

- **Amazon Inspector** is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices.
- **AWS IAM Access Analyzer** helps us to identify the resources in the organization, such as Amazon S3 buckets or IAM (Identity Access Management) roles, that are shared with an external entity. This lets us identify unintended access to our resources and data, which is a security risk.
- **Additionally**, we periodically monitor AWS Trusted advisor findings to keep best practices for cost management, high availability, security, and performance.

CONFIGURATION MANAGEMENT

Automation drives Y Soft's ability to scale with our customers' needs. Server instances are tightly controlled from provisioning through deprovisioning, ensuring that deviations from configuration baselines are detected and reverted at a predefined cadence. If a production server deviates or drifts from the baseline configuration, it will be overwritten with the baseline configuration within 30 minutes.

All server type configurations are embedded in images and configuration files. Server-level configuration management is handled using these images and configuration scripts when the server is built. Changes to the configuration and standard images are managed through a controlled change management process. Each instance type includes its own hardened configuration, depending on the deployment of the instance.

Patch management is handled using automated configuration management tools or by removing server instances that are no longer compliant with the expected baseline and provisioning a replacement instance in its place. Rigorous and automated configuration management is baked into our day-to-day infrastructure processing.

ALERTING AND MONITORING

We also invest heavily in automated monitoring, alerting and response capabilities to continuously address potential issues. The Y Soft product infrastructure is instrumented to alert engineers and administrators when anomalies occur. In particular, error rates, abuse scenarios, application attacks, and other anomalies trigger automatic responses and alerts to the appropriate teams for response, investigation, and correction. As unexpected or malicious activities occur, automated systems bring in the right people to ensure that the issue is rapidly addressed.

Many automated triggers are also designed into the system to immediately respond to unforeseen situations. Traffic blocking, quarantine, process termination, and similar functions kick in at predefined thresholds to ensure that the Y Soft platform can protect itself against a wide variety of undesirable situations.

NETWORK REQUIREMENTS

This section provides information about ports and protocols that must be enabled on firewalls and other related security aspects to ensure safe usage of the solution.

BANDWIDTH AND LATENCY

Bandwidth and latency must be considered for each implementation:

- Latency is important to be kept under 100ms for metadata synchronization in Site Server cluster locations and for user experience on all browser-based terminals (i.e., between where the MFD is and its respective Terminal Server).
- The bandwidth required is vastly dependent on print job data size. Print job metadata traveling among components average around 40–60 kB per print job.

NETWORK COMMUNICATION OVERVIEW

A complete list of the ports and protocols that must be enabled on firewalls to ensure system functionality can be found in the Y Soft SafeQ Cloud documentation. The customer network is expected to allow access to below mentioned services over the Internet, including name resolution (DNS).

Application Protection

DEVELOPMENT

Y Soft recognizes the importance of application security to its customers and is dedicated to bringing products to market that meet high security standards. To meet the high levels of security, Y Soft has partnered with Security Innovation Inc who has assessed the entire software development lifecycle (SDLC) and help defining security practices and activities for the development organization of the YSoft SAFEQ Cloud.

We use OWASP (Open Web Application Security Project) guidelines for software design, vulnerability assessment and threat modelling. Possible security implications are identified and marked during design phase, the code is tested using static and dynamic code tools and analysis. Features with security tags are tested by the QA team and only released if passed.

Y Soft uses secure and mature coding languages for software development. Secure coding guidelines for specific languages are also used by the development teams. Software security is mandated by Y Soft Software Development Security Standard.

The Y Soft Secure Software Development Life Cycle for YSoft SAFEQ Cloud, has been reviewed and SD PAC certified by Security Innovation Inc.

SECURE SOFTWARE DEVELOPMENT LIFECYCLE PROCESS

The product security starts with its design and development. We follow agile product development process and OWASP Software Assurance Maturity Model (SAMM)

Governance	Strategy and Metrics Policy and Compliance	At Y Soft, there are two core business master-processes: Product Development Y Soft is a technology company. Both founders are software engineer (by heart and by experience) and our original 100% indirect business model was a cautious decision, that allowed us to focus more on engineering rather than sales. As the company grows, the focus on marketing and sales is logically increasing, but with ~27% of employees in R&D, its heart remains technological. That said, Product Development is one of our two most important, companywide, business processes. Global Operational Excellence (GOE) Is about how we quote, consult, sell, implement, and support products we have developed using the process above. GOE (or in general product sales, delivery, and support) is our second companywide core process.

		(Product) Marketing While we think that product development is about engineers, in fact it all starts with marketing. They are the ones, who: identify customers' pains and problems, create business cases and calculate return on investment, tell the world, what have we done. What good is a great technology if no one know about it? What good is a great technology if it does not solve real problem?
	Education and Guidance	We continuously educate our engineering teams in terms of security. Regular Community of Practice (CoP) and Dedicated Security Coach role has been established for this matter. Complete development process is documented in the key company document "The Product Development Guidebook," overseen by the CEO of the company. At Y Soft, we have standardized on LeSS and LeSS Huge frameworks, which are based on Scrum. We also follow Agile principles. Y Soft's R&D operates in a manager-less structure, organized per-product. Product organizations are hierarchically flat, i.e., all people within the product report to the Head of Product (up to hundreds of employees reporting to one manager).
Design	Threat Assessment	The Threat Assessment (TA) practice focuses on identifying and understanding of project-level risks based on the functionality of the software being developed and characteristics of the runtime environment. From details about threats and likely attacks against each project, the organization as a whole operates more effectively through better decisions about prioritization of initiatives for security. Additionally, decisions for risk acceptance are more informed, therefore better aligned to the business. STRIDE modelling is a regular part of the development process for all product increments

	Security Requirements and Security Architecture	Secure Architecture Design looks at the selection and composition of components that form the foundation of your solution, focusing on its security properties.
Implementation	Secure Build	Giflow is an alternative Git branching model that involves the use of feature branches and multiple primary branches. Under this model, developers create a feature branch and delay merging it to the main trunk branch until the feature is complete. Mandatory cross team peer review and tooling such as SonarQube and OWASP scans are performed upon every pull request as part of automated build pipelines. All builds are processed by centralized tooling without access of individual developers.
	Secure Deployment	Our deployment process focuses on removing manual error by automating the deployment as much as possible and making its success contingent upon the outcomes of integrated security verification checks. It also fosters Separation of Duties by making adequately trained, non-developers responsible for deployment. Deployment process is staged, providing at least 4 independent checkpoints between build, development environment deployment, staging, quality control environment, pre-production, external QA and production.
	Security Testing	STRIDE analyses are reviewed at the end of every development sprint and feed back to the development.

RELEASE MANAGEMENT

One of Y Soft's greatest advantages is a rapidly advancing feature set, and we constantly optimize our products through a modern continuous delivery approach to software development.

New code is proposed, approved, and merged thousands of times daily. Code reviews, testing (where applicable), and merge approval is performed before deployment. Approval is controlled by designated repository owners. Once approved, code is automatically submitted to Y Soft's continuous integration environment where compilation, packaging and unit testing occur.

All code deployments create archives of existing production-grade code in case failures are detected by post-deploy hooks. The deploying team manages notifications regarding the health of their applications. If a failure occurs, rollback is immediately engaged.

We use extensive software gating and traffic management to control features based on customer preferences (private beta, public beta, full launch). Y Soft features seamless updates, and as a SaaS application, scheduled maintenance windows in relation to new releases. Major feature changes are communicated through pre-release and post release product update posts.

Newly developed code is first deployed to the dedicated and separate Y Soft pre-production environment for the last stage of load testing before being promoted to production. Network-level segmentation prevents unauthorized access between pre-production and production environments.

VULNERABILITY SCANNING AND PENETRATION TESTING

Y Soft manages a multi-layered approach to vulnerability scanning, using a variety of industry-recognized tools to ensure comprehensive coverage of our technology stack.

Vulnerability scans are configured to scan for exploitable vulnerabilities on a regular basis. Continually running scans, using adaptive scanning inclusion lists, and continuously updating vulnerability detection signatures helps Y Soft stay ahead of many security threats.

According to our Software Security Development standard and our Security testing standard, Y Soft has implemented industry best practices for secure SDLC including formal design reviews, code reviews, threat modelling and scanning of the code during development.

We also bring in industry-recognized third parties to perform quarterly penetration tests. The goal of these programs is to iteratively identify flaws that present security risk and rapidly address any issues. Penetration tests are performed against the application layers and network layers of the Y Soft technology stack addressing the OWASP Top 10 and other common Application Security Risk. Schedule of penetration testing is mandated by the Y Soft Security Testing standard.

The results from all Penetration tests are being evaluated by the Y Soft Cloud Operations and Security team, discussed, and prioritised according to the risk score with the Product Management team. Remediations are then planed and implemented. According to the ISO27001 risk assessment framework, all critical issues are also added to our Risk Treatment table and have the attention of the YSoft Information Security Steering Committee.

The content of the PEN Testing reports is highly sensitive information and considered confidential. We do NOT share PEN Testing reports with anyone outside Y Soft. In exceptional cases we might consider sharing a redacted version of our PEN Tests against a signed NDA (Non-Disclosure Agreement).

Customer Data Protection

CONFIDENTIAL INFORMATION

Confidentiality of customer data is a prerequisite and the top priority for any business implementing a cloud-based print management application. The architecture of YSoft SAFEQ Cloud and the technical and organizational measures and controls implemented by Y Soft ensure that the confidentiality of customer data is maintained at the level matching fully on-premises alternatives.

LOGICAL TENANT SEPARATION

Y Soft provides a highly scalable, multi-tenant SaaS solution. The Y Soft user interface and APIs (Application Programming Interface) restrict access to authorized content exclusively. Y Soft logically segments the data using portal IDs and associates that unique ID with all data and objects specific to a customer. Information is made available via the user interface or APIs to be produced for a specific Y Soft portal, without the risk of cross-portal access or data pollution.

Authorization rules are incorporated into the design architecture and validated on a continuous basis. Additionally, we log application authentication and associated changes and application availability.

ENCRYPTION IN-TRANSIT AND AT-REST

All sensitive interactions with the Y Soft products (e.g., API calls, authenticated sessions, etc.) are encrypted in transit with TLS version 1.3 and 2,048 bit keys or better.

Y Soft leverages several technologies to ensure stored data is encrypted at rest. Platform data is stored using AES-256 encryption. User passwords are hashed following industry best practices and are encrypted at rest. Certain email features work by providing an additional level of both at-rest and in-transit encryption.

KEY MANAGEMENT

Encryption keys for both in transit and at rest encryption are securely managed by the Y Soft platform. TLS private keys for in transit encryption are managed through our content delivery partner. Volume and field level encryption keys for at rest encryption are stored in a hardened Key Management System (KMS). Keys are rotated at a frequency that is dependent upon the sensitivity of the data they are encrypting.

Data Backup and Disaster Recovery

SYSTEM RELIABILITY AND RECOVERY

Y Soft is committed to ensuring the availability of our systems by using commercially reasonable efforts to meet a Service Uptime of 99.9% for our Services in each calendar month. Please reference to our Service Level Agreement for more details.

Additionally, we provide real-time updates and historical data on system status and security via Y Soft's status site.

All Y Soft product services are built with full redundancy. Server infrastructure is strategically distributed across multiple distinct availability zones and virtual private cloud networks within our infrastructure providers, and all web, application, and database components are deployed with a minimum of n+1 supporting server instances or containers.

DISASTER RECOVERY

Y Soft maintains a disaster recovery plan that is tested quarterly as a part of our ISO27001 controls.

BACKUP STRATEGY

SYSTEMS BACKUP

Systems are backed up regularly with established schedules and frequencies. Several days' worth of backups are kept for any database in a way that ensures restoration can occur easily. Backups are monitored for successful execution, and alerts are generated in the event of any exceptions. Failure alerts are escalated, investigated, and resolved.

Data is backed up daily to their local region. Additionally, backups are copied periodically to off-site locations in the event of a primary regional outage. Monitoring and alerting are in place for replication failures and triaged accordingly. During the restore tests, we use a checklist to determine all the items that need to be tested to confirm that the DR test was successful. Our Recovery Point Objective is maximum 24 hours and SLO for Recovery Time Objective, RTO is 90 min.

All production data sets are stored on a highly available file storage facility like Amazon's S3.

PHYSICAL BACKUP STORAGE

Because we leverage public cloud services for hosting, backup, and recovery, Y Soft does not implement physical infrastructure or physical storage media within its products. Y Soft does not generally produce or use other kinds of hard copy media (e.g., paper, tape, etc.) as part of making our products available to our customers.

BACKUP PROTECTIONS

By default, all backups are encrypted and protected through access control restrictions on Y Soft product infrastructure networks and access control lists on the file systems storing the backup files.

Identity and Access Control

PRODUCT USER MANAGEMENT

The Y Soft products allow for granular authorization rules. Customers are empowered to create and manage users of their portals and assign the privileges that are appropriate for their accounts and limit access to their data features.

For more information about user roles, please see the Y Soft SafeQ Cloud documentation.

PRODUCT LOGIN PROTECTIONS

The Y Soft products allow users to login to their YSoft SAFEQ Cloud accounts using built-in login or Single Sign On (SSO). The built-in login enforces a uniform password policy which requires a minimum of 6 characters and a combination of lower- and upper-case letters, special characters, whitespace, and numbers. People who use Y Soft's built-in login cannot decrease the default password length and have the ability to enforce more secure password policies if required.

More advanced SAML-based SSO integrated with any SAML-based IDP is available.

Customers who use an SSO provider can set up SSO-based login for their users. Instructions for setting up SSO are available in the YSoft SAFEQ Cloud documentation and Y Soft Academy. Single Sign On users can configure a password policy in their SSO provider.

PRODUCT API AUTHORIZATION

Application programming interface (API) access is enabled through either API keys or Oauth (version 2) authorization. Customers can generate API keys for their portals. The keys are intended to be used to rapidly prototype custom integrations. Y Soft's Oauth implementation is a stronger approach to authenticating and authorizing API requests. Additionally, Oauth is required of all featured integrations. Authorization for Oauth enabled requests is established through defined scopes.

PRODUCTION INFRASTRUCTURE ACCESS

Access to Y Soft's systems is strictly controlled and follows the principle of least privilege. Y Soft employees are granted access using a role-based access control (RBAC) model.

Day to day access is minimized to only the individuals whose jobs require it. For emergency access (e.g., alerts responses/troubleshooting) and access to administrative functions, Y Soft's system uses a Just-In-Time-Access (JITA) model in which users can request access to privileged functions for a limited duration. Each JITA request is logged, and logs are continuously monitored for anomalous requests. After the configured session limit, access to the account expires and is automatically revoked.

Employee access to both corporate and production resources is subject to daily automated review and at least semi-annual manual recertification.

Y SOFT EMPLOYEE ACCESS TO CUSTOMER PORTALS

Customer Support, Services, and other customer engagement staff may request JITA to customer portals on a time limited basis. Requests for access are limited to their work responsibilities associated with supporting and servicing our customers. All access requests, logins, queries, page views and similar information are logged.

CORPORATE AUTHENTICATION AND AUTHORISATION

Access to the Corporate network, both remotely and while in office, requires multi factor authentication (MFA), and any SaaS applications in use by Y Soft require SSO with MFA to facilitate centralized access control.

Password policies follow industry best practices for required length, complexity, and rotation frequency.

We built an extensive set of support systems to streamline and automate our security management and compliance activities. In addition to many other functions, the system sweeps our product and corporate infrastructure several times daily to ensure that permission grants are appropriate, to manage employee events, to revoke accounts and access where needed, to compile logs of access requests, and to capture compliance evidence for each of our technology security controls. These internal systems sweep the infrastructure validating that it meets approved configurations on a 24-hours basis.

Organisational and Corporate Security

BACKGROUND CHECKS AND ONBOARDING

Y Soft employees undergo a background check prior to formal employment offers. Employment, education, and criminal checks are performed for potential employees. Reference verification is performed at the hiring manager's discretion.

Upon hire, all employees must read, and acknowledge Y Soft's Information Security Policy and IT Acceptable Use Policy which help define employee's security responsibilities in protecting company assets/data (including, but not limited to protecting mobile devices, and securing corporate equipment).

POLICY MANAGEMENT

To help keep all our employees on the same page regarding protecting data, Y Soft documents and maintains several written policies and procedures. Y Soft maintains a core Written Information Security Policy - the policy covers data handling requirements, privacy considerations, and responses to violations, among many other topics.

Policies are reviewed and approved at least annually and stored in the company wiki. Policies requiring acknowledgment by employees are incorporated into mandatory annual training.

SECURITY AWARENESS TRAINING

We consider employees to be our first line of defense and we ensure Y Soft employees are well trained for their roles. Security awareness training that covers general security best practices is offered to all new Y Soft employees upon hire, and on an annual basis. In addition to awareness training, Y Soft keeps employees aware of recent security news or initiatives with internal knowledge articles.

After initial training, more specialized content is available based on an employee's role or resulting access. For example, Y Soft has a Security Champions program, where developers on the product teams have opportunities for additional training on security development, common risk, threats, and issues.

RISK MANAGEMENT

Within Y Soft a Risk Register has been created which identifies hazards encountered during the company's operations. Managers are encouraged to populate this register with hazards that have not previously been identified within their respective project area. This register is held on Y Soft Confluence. This document forms part of overall Y Soft's Information Security Management Systems Framework.

Risk mitigation and remediation activities are tracked via a ticketing system and reviewed at a designated cadence.

VENDOR MANAGEMENT

We leverage several third-party service providers who augment the Y Soft products' ability to meet your marketing, sales, services, content management, and operational needs. We maintain a vendor management program to ensure that appropriate security and privacy controls are in place. The program includes inventorying, tracking, and reviewing the security programs of the vendors who support Y Soft.

Appropriate safeguards are assessed relative to the service being provided and the type of data being exchanged. Ongoing compliance with expected protections is managed as part of our contractual relationship with them. Our Security, Legal, and Compliance teams coordinate with our business stakeholders as part of the vendor management review process.

CORPORATE PHYSICAL SECURITY

Y Soft offices are secured in multiple ways. Security guards are employed at each of Y Soft's global locations to help create a safe environment for Y Soft employees. Door access is controlled using RFID tokens tied to individuals, which are automatically deprovisioned if lost or when no longer needed (e.g., employee termination, infrequent use, etc). Video surveillance, and many other protective measures are implemented across Y Soft offices.

CORPORATE NETWORK PROTECTIONS

Centrally managed application firewalls are deployed for High Availability at Y Soft Corporate offices. Our guest networks are separate from our corporate network and are serviced by separate firewalls. Firewalls are set up to filter unauthorized inbound traffic from the Internet and are configured to deny inbound network connections that are not explicitly authorized by a rule.

Y Soft enforces system compliance checks prior to authorizing a device's connection to the corporate network. Unauthorized devices are disconnected immediately or moved to containment VLANs.

ENDPOINT PROTECTION AND ANTIVIRUS/MALWARE PROTECTION

Y Soft leverages different endpoint protection solutions to protect its systems. These enables us to have extensive visibility into anomalous system behaviour as well as to rapidly investigate and take appropriate action through either automated event triggers or manual containment of a system.

Incident Management

INCIDENT RESPONSE

Y Soft's Cloud Operations and Security team respond quickly to all security and privacy events. Y Soft's rapid incident response program is responsive and repeatable. Pre-defined incident types, based on historical trending, are created to facilitate timely incident tracking, consistent task assignment, escalation, and communication. Many automated processes feed into the incident response process, including malicious activity or anomaly alerts, vendor alerts, customer requests, privacy events, and others.

In responding to any incident, we first determine the exposure of the information and determine the source of the security problem, if possible. We provide periodic updates as needed to ensure appropriate resolution of the incident.

Our Chief Security Officer reviews all security-related incidents, either suspected or proven, and we coordinate with affected customers using the most appropriate means, depending on the nature of the incident.

Compliance

Y Soft adheres to domestic and international information security standards, as well as industry requirements. We integrate compliance requirements and standards into our internal control framework and implement such requirements and standards by design in our cloud print service. We are also engaging with independent third parties to verify the compliance of Y Soft according to various requirements. Our framework and compliance foundations are based on the following:

INFORMATION SECURITY STANDARDS

Y Soft leverages best practices and sound security guidance from a wide variety of sources. The best practices that we consider as we continuously improve our security programs include the Cloud Security Alliance's Cloud Control Matrix, ISO27001, SD-PAC for our Secure SDLC from Security Innovation Inc. and several others.

Y Soft considers all information, applications and underlying IT infrastructure as important assets which are supporting business processes and are being adequately protected. The scope of our IT risk includes the potential loss of confidentiality, integrity, and availability of information assets due to inadequate controls or exploitation of security vulnerabilities. Our Policy framework is approved by the Chief Executive Officer on behalf of the Executive Management at Y Soft and provides a management statement highlighting the key IT Security Principles for managing IT risk.

ISO/IEC 27001 CERTIFIED

Our Cloud infrastructure is governed by our ISO/IEC 27001 certification, the internationally recognised standard for information security management systems (ISMS). ISO 27001 accreditation provides independent assurance that systems are designed and operated with cloud-first security principles and that robust processes are in place to build resilience and help avoid potential data security issues.

Our compliance with this internationally recognised standard proves the completeness and strength of our security controls and provides an independently verified assurance of our systematic approach to managing our cloud environment and demonstrates that robust processes are in place to build resilience and help avoid potential data security issues.

Access to our production environment is securely protected and regulated according to strict ISO27001 standards and procedures.

CLOUD SECURITY ASSOCIATION, CSA

We also use the Cloud Controls Matrix (CCM) control framework to align our cyber security to the Cloud Security Association, CSA best practices, that is considered the de-facto standard for cloud security and privacy. CAIQ Self-assessment has been done and can be shared under NDA.

DATA PROTECTION LAWS

Y Soft maintains full GDPR (General Data Protection Regulation) compliance across Y Soft's regional subsidiaries and other suppliers engaged in personal data processing, except for the hosting providers, who offer a GDPR-compliant regime based on the hosting region selected by the customer.

GDPR compliance in the form of the data minimization principle projects itself to the core product architecture that ensures personal data and other sensitive information contained in print and scan jobs remain safely in the customer environment.

Y Soft has appointed a Data Protection Officer (DPO) to meet its commitment to data protection and compliance with data protection regulations. The DPO is responsible for ensuring that Y Soft's processing of personal data complies with GDPR and other applicable data protection laws.

To help its customers achieve GPDR-compliant personal data processing, Y Soft offers a range of legal and technical tools such as an option to host data at rest in EU/EEA, DPA (Data Processing Agreement) implementing the latest compliant data transfer mechanisms and assistance to customers with responding to personal data subject requests including data access requests, data rectification requests, and data deletion requests. By providing these tools and measures, Y Soft empowers the customers to maintain compliance with GPDR and any applicable data protection laws.

The privacy of our customers' data is one of Y Soft's primary considerations. The protections described in this document and other protections that we have implemented are designed to ensure that your data stays private and unaltered. The Y Soft products are designed and built with customer needs and privacy considerations in the forefront. Our privacy program incorporates best practices, customers,' and their contacts' needs, as well as regulatory requirements.