Yarken Security and Business Continuity Framework

OCTOBER 2022 – VERSION 1.0

YäRKEN.

Connecting the dots between
IT and finance.

www.yarken.com

YäRKEN.

Table of Contents

1 Copyright information

This document is published and distributed by Yarken. The information contained in this document is protected under copyright, furnished for informational use only, and is subject to change without notice at any time.

This material represents substantial creative effort and contains confidential information, as well as other proprietary concepts, techniques, ideas, and expressions. This material may not be changed, distributed, reproduced, or shared in any form or by any means (including but not limited to, digital, electronic, mechanical, or hard copy), without the prior express written consent of Yarken.

Your possession or use of this material constitutes your acceptance of these conditions. If you do not agree with these conditions, please return the material to Yarken.

2 Framework

Yarken takes information security seriously and has established a policy framework focused on protecting the confidentiality, integrity, and availability of the information assets of both our customers and our company. We have establishing security standards identifying reasonably foreseeable security risks, minimizing risks through risk assessment and regular testing, and enforcing internal policies and procedures.

2.1 People

All Yarken employees receive security and privacy awareness training annually. Attendance to these trainings is recorded.

2.2 Identity and Access Management

2.2.1 Account and Password Standards

Yarken Accounts and access are grafted with the principle of least privilege in all cases, ensuring that only those who are responsible for, or working directly with, a resource have access to that resource at any given point in time.

Extra controls are in place to prevent unauthorised access to customer data.

All internal accounts and passwords follow best practise outlined in Yarken's Account and Password policy.

2.2.2 Physical Security

Yarken hosts its applications in cloud environments that meet the following compliance standards:

> *CIS Benchmark, CSA STAR Attestation, CSA STAR Certification, CSA STAR Self-Assessment, ISO 20000, ISO 22301, ISO 27001, ISO 27017, ISO 27018, ISO 27701, ISO 9001, SOC 1, SOC 2, SOC 3, WCAG 2.0*

Data Centres used are geographically separated across the globe and have physical access controls in place to prevent unauthorised access.

2.2.3 Encryption & Key Management

Yarken uses industry-standard encryption and key management systems to protect customer Data while in storage and during transmission, including through Transport Layer Encryption (TLS 1.2 or above) leveraging at least 2048-bit RSA server certificates and 256-bit symmetric encryption keys at a minimum.

2.2.4 Anti-Virus/Anti-Malware

All Yarken Windows workstations use virus and malicious code detection and protection products consistent with industry standards.

2.2.5 Secure Disposal

Yarken implements processes to ensure the appropriate destruction/re-use of assets including the prior destruction of customer data.

2.2.6 Network Security

Yarken applies industry best practises to prevent disclosure of customer Data to any person not having a need to know of or access to such information.

Yarken maintains access controls and policies to manage access from each network connection including the use of firewalls or functionally equivalent technology.

Least privilege-based authentication and authorization controls are maintained and periodically reviewed to ensure that access can only be granted to Yarken personnel whose function and/or duties justifies such access.

Some of the additional systems in place to maintain a strong and robust security infrastructure include IDS, centralized log management and comprehensive alerting.

All inbound traffic is routed and filtered to more secure network segments.

2.2.7 Intrusion Detection, Logging & Monitoring

Yarken creates log records to the extent needed to enable monitoring, analysis, investigation, and reporting of information system activity, including successful and unsuccessful account logon events, account management events, security events, object access, IDS/IPS logs, firewall logs, and permission changes.

2.3 Secure Application Development

2.3.1 Secure Application Architecture

Yarken utilizes a multi-tier architecture which segregates the web service and application layers from the database layer, with each layer firewalled and limited from other layers via access control lists or security groups.

All Data is encrypted at rest and logically isolated from other Yarken customers by deploying individual database instances per customer.

Internet traffic in connection with our services is encrypted with HTTPS/TLS with AES256 bit encryption and related application authentication is performed over this connection; weaker encryption ciphers are not supported.

Yarken delegates user identification to customer's Azure Active Directory and therefore does not store passwords. Customers' authentication policies like two factor authentication apply.

2.3.2 Secure Application Development

Security is front of mind during the entire software development life cycle. All check-ins are peer reviewed and are manually and automatically assessed using state of the art SAST and DAST tooling and processes. Vulnerabilities are remediated prior to production deploy.

2.3.3 Third Party Components

Yarken's development and quality assurance teams assess known vulnerabilities in all 3rd party components prior to each production deploy on a risk basis and relevance to the Yarken product and remediates findings by upgrading, downgrading, replacing and/or changing the usage of such components.

2.3.4 Vulnerability Management and Penetration Testing

Yarken conducts regular internal and external scans for network and system vulnerabilities of Yarken applications.

Yarken uses a risk-based approach to determine the timing for remediation of the vulnerabilities and remediates or mitigates critical or high-risk vulnerabilities in accordance with Yarken policies.

Yarken retains a qualified third party to conduct network penetration and application vulnerability testing of Yarken's infrastructure on an annual basis.

The scope includes OWASP Top 10 among other potential threat vectors. All findings are assessed and remediated according to the finding's severity level.

2.3.5 Third-Party Security Assessment

Third party access to customer's data as part of Yarken's applications and services is not permitted.

Yarken uses Azure Data Centres to host Yarken applications and to store customers' encrypted data as part of its data centre and public cloud use only. Third parties are vetted regarding the security posture prior to use.

2.4 Incident Management and Incident Response

If a verifiable information systems security problem, or a suspected but likely information security problem, has caused third party private or confidential information to be exposed to unauthorized persons, unless required by law, regulation, or contractual obligation otherwise, these third parties will be immediately informed about the situation.

Yarken will take commercially reasonable measures to address the issue in a timely manner.

2.5 Business Continuity

2.5.1 Business Continuity

Yarken policies mandate the implementation and assessment of a business continuity plan. The plan

- Identifies Yarken's key products and services
- Identifies key staff
- Documents key connections
- Lists essential equipment and supplies
- Considers relocation options
- Considers insurance options
- Keeps contact details handy
- Ensures important data is backed up

2.5.2 Disaster Recovery

Yarken maintains a Disaster Recovery plan that ensures that should a disaster be declared Yarken's services are relocated to a back-up system and/or data centre and are operational with following two key objectives:

RPO (Recovery Point Objective): 24 hours.

This means that in the event of a declared disaster that requires failover to alternate data centre or availability zone, the target objective is that not more than the most recent 24 hours of customer's Data will be lost.

RTO (Recovery Time Objective): 48 hours.

This means that in the event of a declared disaster, the target objective is that customer's Data will be recovered to an alternate site within 48 hours.

2.6 Audit and Compliance

To ensure compliance with Yarken policies and to ensure security, integrity, and availability for our customer, Yarken performs annual evaluation of its policies and procedures directly and via third-party audits.

Yarken's security policies are subject to change as Yarken's information security practices will evolve over time to keep pace with appropriate industry standards.

3 Revision History

Date of Change	Version	Summary of Change
05/10/2022	1.0	Initial Version