harvest Security Self Assessment Questionnaire

We use this questionnaire as a baseline mechanism to express our security posture in real terms and to provide security control transparency.

Section Heading	Control Heading	ID	Question Text	Ans	Notes/Comment
Application & Interface Security	**Application Security**	AIS-01.2	Do you use an automated source code analysis tool to detect security defects in code prior to production?	Yes	Source code analysis scans are run automatically on code changes to detect security vulnerabilities as part of our continuous integration process.
		AIS-01.5	(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	Yes	Security issues found during review or testing are fixed prior to deployment to production.
	Customer Access Requirements	AIS-02.1	Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and information systems?	Yes	Our legal policies regarding the usage and access to customer data are available at: https://www.getharvest.com/privacy-policy
	Data Integrity	AIS-03.1	Does your data management policies and procedures require audits to verify data input and output integrity routines?	Yes	We check the validity of data input prior to ingestion and to sanitize all outputs. We have tests, static security code scanning tools and human review. All data schema migrations need to follow standard code review procedures.
Audit Assurance & Compliance	**Independent Audits**	AAC-02.1	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or	Yes	We rely on our server host's audit, and they are SOC 2 and ISO 27001 certified.

			certification reports?		
		AAC-02.2	Do you conduct network penetration tests of your cloud service infrastructure at least annually?	Yes	We run a public bug bounty security program. We are under a 24/7 security audit performed by the people participating in the program, and we have contracted commercial penetration tests in the past.
		AAC-02.3	Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	Yes	See previous answer
	Information System Regulatory Mapping	AAC-03.1	Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?	Yes	We regularly review the regulatory landscape and make changes to our internal policies and documentation as a result.
Business Continuity Management & Operational Resilience	**Business Continuity Testing**	BCR-02.1	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	Yes	Our business continuity plan is reviewed annually or if major changes occur within the business.
	Policy	BCR-10.1	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	Yes	We continuously update our public documentation, our internal documentation and staff training material. All policies and procedures are available to all employees.
	Retention Policy	BCR-11.1	Do you have technical capabilities to enforce tenant data retention policies?	Yes	We have technical controls enforcing data retention policies.

		BCR-11.3	Have you implemented backup or recovery mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	Yes	All backups are replicated to at least 2 physical data centers. All backup systems are tested biweekly. Backups occur multiple times per day, and are retained for 180 days.
		BCR-11.7	Do you test your backup or redundancy mechanisms at least annually?	Yes	Backups are tested daily.
Change Control & Configuration Management	**Unauthorized Software Installations**	CCC-04.1	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	Yes	We automate the provisioning of infrastructure we use to deliver our services. We only rely on trusted sources, access to systems is monitored.
Data Security & Information Lifecycle Management	**E-commerce Transactions**	DSI-03.1	Do you provide standardized (e.g. ISO/IEC) non-proprietary encryption algorithms (3DES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?	Yes	All data is encrypted in transit, and all connections use TLS 1.2/1.3. We follow a formal written encryption policy.
		DSI-03.2	Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?	Yes	All data transferred by our infrastructure components is either transferred through private networks or by using encryption via TLS 1.2 and above.
	Nonproduction Data	DSI-05.1	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	Yes	Environments are isolated and data is never shared. Production data is only accessible by support personnel working on our infrastructure.
	Secure Disposal	DSI-07.1	Do you support the secure deletion (e.g., degaussing/cryptographic wiping) of archived and	Yes	All logs and backups are deleted after the retention period. Secure deletion is managed by our datacenter provider.

			backed-up data?		
		DSI-07.2	Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?	Yes	If customers would like to stop using our product, our website makes it easy to cancel or deactivate their account. Data from live databases are deleted shortly after that.
Datacenter Security	**Asset Management**	DCS-01.2	Do you maintain a complete inventory of all of your critical assets located at all sites/ or geographical locations and their assigned ownership?	Yes	All Harvest assets are tracked and owned by the Operations and Security team.
	Controlled Access Points	DCS-02.1	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented for all areas housing sensitive data and information systems?	Yes	All cloud infrastructure is hosted on Google Cloud that implements such physical security measures. We can share the audit report after establishing a non-disclosure agreement (NDA).
	User Access	DCS-09.1	Do you restrict physical access to information assets and functions by users and support personnel?	Yes	See previous answer.
Encryption & Key Management	**Key Generation**	EKM-02.1	Do you have a capability to allow creation of unique encryption keys per tenant?	N/A	Being a SaaS application Harvest does not support unique keys per customer.
	Encryption	EKM-03.1	Do you encrypt tenant data at rest (on disk/storage) within your environment?	Yes	Sensitive database fields are encrypted at rest. Passwords are stored hashed and salted using bcrypt with a work function of 12. Backups are encrypted using the AES-256 cipher. Attachments and other file assets are stored encrypted at rest on Amazon S3.

Governance and Risk Management	**Baseline Requirements**	GRM-01.1	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?	Yes	Our infrastructure provisioning is automated, new infrastructure is built with predefined images following standard security baselines, all changes must undergo code review. We have a written information security policy.
	Policy	GRM-06.1	Are your information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business role/function and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)?	Yes	Our information security policy is available to all employees and follows industry best practices.
	Policy Enforcement	GRM-07.1	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	Yes	These actions are enforced by our employment contracts and defined in our policies.
	Policy Reviews	GRM-09.1	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	Yes	We have public security and privacy policies published on our web. If a change in those policies impacts our customers in a meaningful way we'll communicate via email.
		GRM-09.2	Do you perform, at minimum, annual reviews to your privacy and security policies?	Yes	Annually and every time there is a meaningful change in the way we operate.
Human Resources	**Asset Returns**	HRS-01.1	Upon termination of contract or business relationship, are employees and business partners adequately informed of their obligations for returning organizationally-owned assets?	Yes	We have a thorough and strict departure protocol that is enforced the very same day an employee leaves the company including returning organizationally-owned assets.

	Background Screening	HRS-02.1	Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification?	Yes	We perform basic background checks on candidates.
	Employment Agreements	HRS-03.1	Do your employment agreements incorporate provisions and/or terms in adherence to established information governance and security policies?	Yes	Our new hires are inducted with a security awareness program, and we follow up regularly with automatic checks.
	Employment Termination	HRS-04.1	Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination?	Yes	Upon employee termination, all employee devices need to be returned by the termination date. Accounts are closed by the termination date. For the few shared accounts that we're unable to avoid, all passwords are changed to ensure that the terminated employee no longer has access.
	Training / Awareness	HRS-09.5	Are personnel trained and provided with awareness programs at least once a year?	Yes	At least twice per year.
Identity & Access Management	**Audit Tools Access**	IAM-01.1	Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)?	Yes	All live infrastructure access is restricted to support personnel which needs to manage our live infrastructure. All access to our live infrastructure is logged, monitored, and indexed in multiple places.
		IAM-01.2	Do you monitor and log privileged access (e.g., administrator level) to information security management systems?	Yes	All access is logged, monitored, and indexed. We have alerts set for suspicious activity.
	User Access	IAM-02.1	Do you have controls in place	Yes	We follow the Principle of Least Privilege actively

	Policy		ensuring timely removal of systems access that is no longer required for business purposes?		removing access when it is not needed anymore.
	Policies and Procedures	IAM-04.1	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	Yes	We know the level of access to systems and internal tools. All access is logged.
	Source Code Access Restriction	IAM-06.1	Are controls in place to prevent unauthorized access to your application, program, or object source code, and assure it is restricted to authorized personnel only?	Yes	Access to our infrastructure is only provided for developers. Source code is managed within GitHub and we only allow access to authorized personnel.
		IAM-06.2	Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to authorized personnel only?	N/A	We are a SaaS, our customers are only able to access Harvest via web and official apps.
	User Access Restriction / Authorization	IAM-08.1	Do you document how you grant, approve and enforce access restrictions to tenant/customer credentials following the rules of least privilege?	Yes	Access to customer data is restricted to our live infrastructure. It is only granted to support personnel working on our live infrastructure and access is documented internally.
	User Access Reviews	IAM-10.1	Do you require a periodical authorization and validation (e.g. at least annually) of the entitlements for all system users and administrators (exclusive of users maintained by your tenants), based on the rule of least privilege, by business leadership or other accountable business role or function?	Yes	Accounts and access are reviewed by the security team more than once per year.

	User Access Revocation	IAM-11.1	Is timely deprovisioning, revocation, or modification of user access to the organizations systems, information assets, and data implemented upon any change in status of employees, contractors, customers, business partners, or involved third parties?	Yes	We have a thorough and strict protocol to revoke access and rotate keys and passwords when needed.
Infrastructure & Virtualization Security	**Audit Logging / Intrusion Detection**	IVS-01.1	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents?	Yes	We don't run any commercial IDS/IPS, but we have in-house alert systems set on our infrastructure and application logs to detect suspicious activity and anomalies. A member of the operations team is always on call.
		IVS-01.2	Is physical and logical user access to audit logs restricted to authorized personnel?	Yes	Access to logs is restricted to authorized personnel.
		IVS-01.5	Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	Yes	We have alerts for suspicious activity running 24/7. Alerts are reviewed regularly by the security and operations teams.
	Clock Synchronization	IVS-03.1	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	Yes	We ensure time-synchronization on all hosts.
	OS Hardening and Base Controls	IVS-07.1	Are operating systems hardened to provide only the necessary ports, protocols, and services to meet business needs using technical controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline build standard or template?	Yes	Our operating systems contain only packages required for our apps to be run and monitored properly. We follow all the standard security procedures.
	Production /		For your SaaS or PaaS offering,	N/A	We're a SaaS-only provider,

	Non-Production Environments	IVS-08.1	do you provide tenants with separate environments for production and test processes?		separate environments for production and test processes doesn't make sense for our customers. We do allow trial accounts to be created without restrictions.
		IVS-08.3	Do you logically and physically segregate production and non-production environments?	Yes	Our production and non-production environments are completely segregated.
	Segmentation	IVS-09.1	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	Yes	Our system and network environments are sufficiently segregated with separate access restrictions to ensure security requirements.
	VMM Security - Hypervisor Hardening	IVS-11.1	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?	Yes	Access to the hosted environment’s administrative console is restricted to authorized personnel only and based on the principle of least privilege.
	Wireless Security	IVS-12.1	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?	N/A	We are a remote company. We don’t own wireless networks.
		IVS-12.2	Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and	N/A	See previous answer.

			transmission, replacing vendor default settings (e.g., encryption keys, passwords, SNMP community strings)?		
		IVS-12.3	Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?	N/A	Being a remote company, we don't own wireless networks to provide or support our products, there is no 'corporate intranet' or in house data center. All access to our production environments requires authentication using two factor authentication over TLS 1.2/1.3 connections or via local private keys protected by password.
Interoperability & Portability	**APIs**	IPY-01.1	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	Yes	We have detailed and updated API documentation available: https://help.getharvest.com/api-v2
Mobile Security	**Approved Applications**	MOS-03.1	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores can be loaded onto a mobile device?	N/A	Harvest does not issue mobile devices to employees to work. Our systems and internal tools require a full size screen in order to be useful.
Security Incident Management, E-Discovery, & Cloud Forensics	**Incident Management**	SEF-02.1	Do you have a documented security incident response plan?	Yes	We have a documented security incident response policy and plan that is reviewed by the security team at least annually.
		SEF-02.4	Have you tested your security incident response plans in the last year?	Yes	See previous answer.
	Incident Reporting	SEF-03.1	Are workforce personnel and external business relationships adequately informed of their responsibility, and, if required, consent and/or contractually	Yes	Our employees are trained in how to communicate incidents internally and our customers will be kept informed of incidents if those affect them.

			required to report all information security events in a timely manner?		In cases that affect a small subset of our customers we may reach out directly to those affected customers.
		SEF-03.2	Do you have predefined communication channels for workforce personnel and external business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations?	Yes	See previous question.
	Incident Response Legal Preparation	SEF-04.4	Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	Yes	All database and log data from our apps can be extracted if needed.
Supply Chain Management, Transparency, and Accountability	**Incident Reporting**	STA-02.1	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?	Yes	Incidents are detailed via our status page at: https://www.harveststatus.com And other sources like email and Twitter if needed.
	Network / Infrastructure Services	STA-03.1	Do you collect capacity and use data for all relevant components of your cloud service offering?	Yes	Multiple tools are used for the tracking of use and capacity data to forecast capacity planning and determine the potential cause of anomalous usage patterns.
	Third Party Agreements	STA-05.4	Do third-party agreements include provision for the security and protection of information and assets?	Yes	Our third-party agreements include security and privacy provisions as applicable.
		STA-05.5	Do you have the capability to recover data for a specific customer in the case of a failure or data loss?	Yes	We are able to recover from backups and logs data for a specific customer in case of failure.
	Supply Chain		Do you provide tenants with ongoing visibility and reporting	N/A	Harvest doesn't offer an SLA or SLA Performance

	Metrics	STA-07.4	of your operational Service Level Agreement (SLA) performance?		monitoring, however we do communicate service disruptions to our status page
	Third Party Audits	STA-09.1	Do you mandate annual information security reviews and audits of your third party providers to ensure that all agreed upon security requirements are met?	N/A	While we review the security of third party providers frequently we do not require annual security reviews to ensure agreed security requirements.
Threat and Vulnerability Management	**Antivirus / Malicious Software**	TVM-01.1	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your IT infrastructure network and systems components?	Yes	Security and vulnerability management for infrastructure is tackled via automated tools that review our source code, and ultimately human review. Employees are required to use Gatekeeper or a similar anti-malware feature and maintain the system updated.
	Vulnerability / Patch Management	TVM-02.5	Do you have a capability to patch vulnerabilities across all of your computing devices, applications, and systems?	Yes	Our infrastructure is patched with automated operating system updates. We also update manually all libraries and external dependencies as we are subscribed to all relevant sources. We use an endpoint security solution to keep all work machines updated and following best practices.
	Mobile Code	TVM-03.1	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?	N/A	We don't issue employees mobile phones or tablets to work.