Honorlock

Vendor Security Cheat Sheet

Questions to ask technology vendors, software and technologies needed, and definitions to know.

Table of Contents

Questions to Ask Technology Vendors

Here are high-level questions to ask vendors during the vetting process:

Data Ownership

- Who owns the data?

Data Encryption

- Is the data encrypted in transit and at rest?

Data Localization

- Where will our data be stored?
- Does it ever leave that country?

Data Classification

- Do you have a data classification policy?
    - Are your employees trained to handle different classifications?

Proactive Defense

- Do you routinely do vulnerability scans, if so what is the cadence?
- Do you routinely do penetration tests, if so what is the cadence?
- How are you integrating security into your design processes?

Incident Response Plan

- Do you have an incident response plan in place?
    - If so, how often do you run through the plan in practice and simulation?

Privacy Policy

- Can you provide a public-facing privacy policy?
- How is data collected and maintained?
- What data is collected?

Employee Security Training

- Do you train employees on security best practices?
    - If so, how often are employees trained?
- Do you test employees in real-world situations?
    - If so, how do you test them and how often?
- When and how are employees trained on reporting a security incident?
- Are your developers trained in secure coding?

Contractor data access

- Will contractors be accessing our data?
- If so, what controls are in place to ensure their security?
- Do you require that they complete NDAs and Background checks?

FERPA Compiance

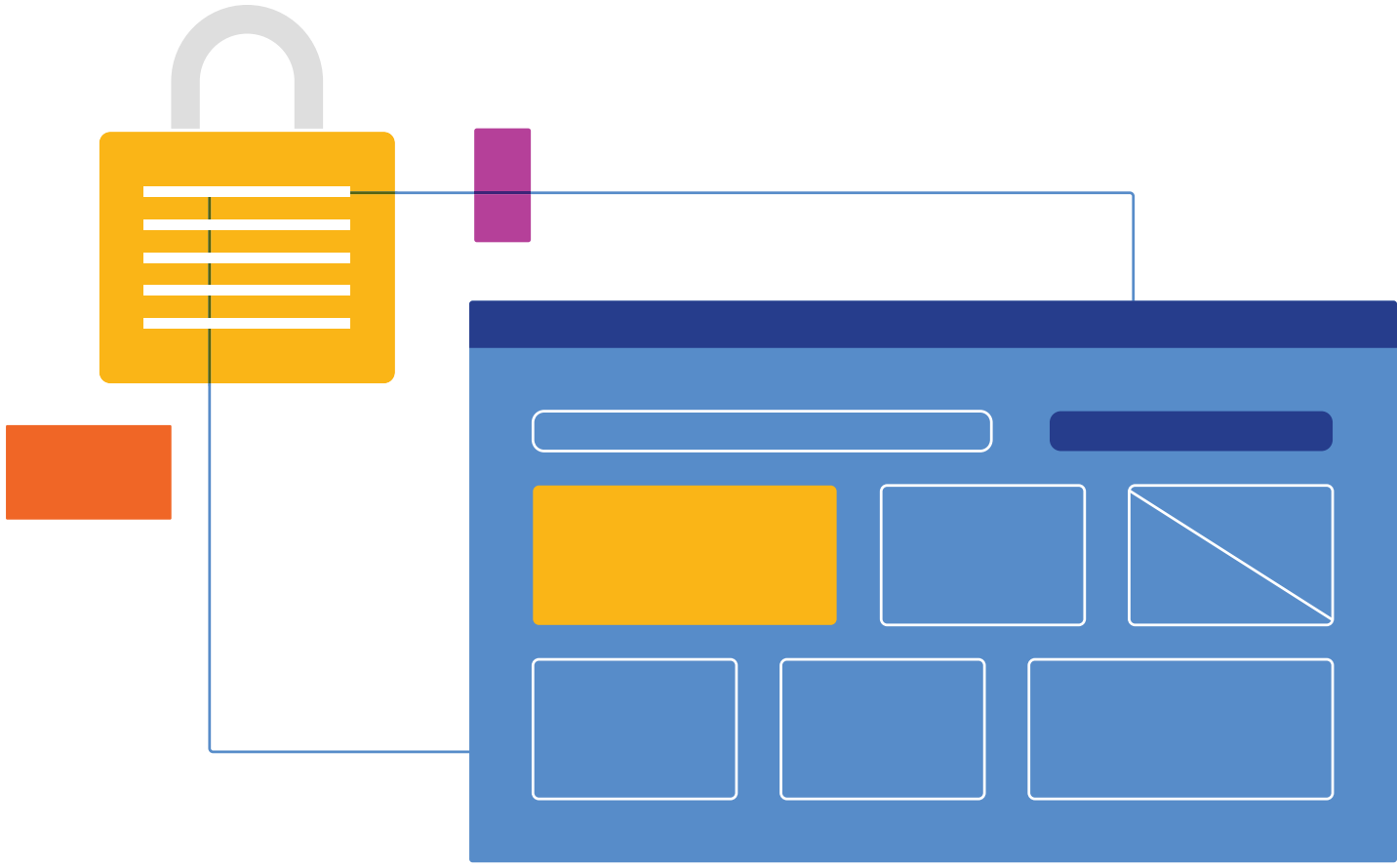
- Is the organization FERPA compliant?

Breach Notification

- In the unfortunate case of a breach how and when will we be notified?
- Have a you had a breach in the last 5 years and if so how was it disclosed?

Information Security Management

- Is information security represented at the executive level
- If not, how does the organization ensure that they have unbiased advisory on security issues?
- How is security prioritized in the software development lifecycle?



Vendor Security Technology Checklist

Does the vendor have the following software and technologies in place:

	Yes	No
Web Application Firewall (WAF)	☐	☐
Intrusion Detection System (IDS)	☐	☐
Antivirus/Anti-Malware	☐	☐
Next Generation Antivirus	☐	☐
Single Sign-on	☐	☐
Multifactor Authentication	☐	☐
Logging tools	☐	☐
Snapshots and backups	☐	☐
Documented Recovery Time & Recovery Point Objective	☐	☐

Vendor Security Assessments

Use this list of vendor security assessments as a starting point for your questions to ask but remember that you'll need to customize your questions and requirements to meet your institution's specific needs.

Consensus Assessments Initiative Questionnaire (CAIQ/CAIQ Lite)

Security control questions that create accepted industry standards and increase transparency.

Vendor Security Alliance Questionnaire (VSA)

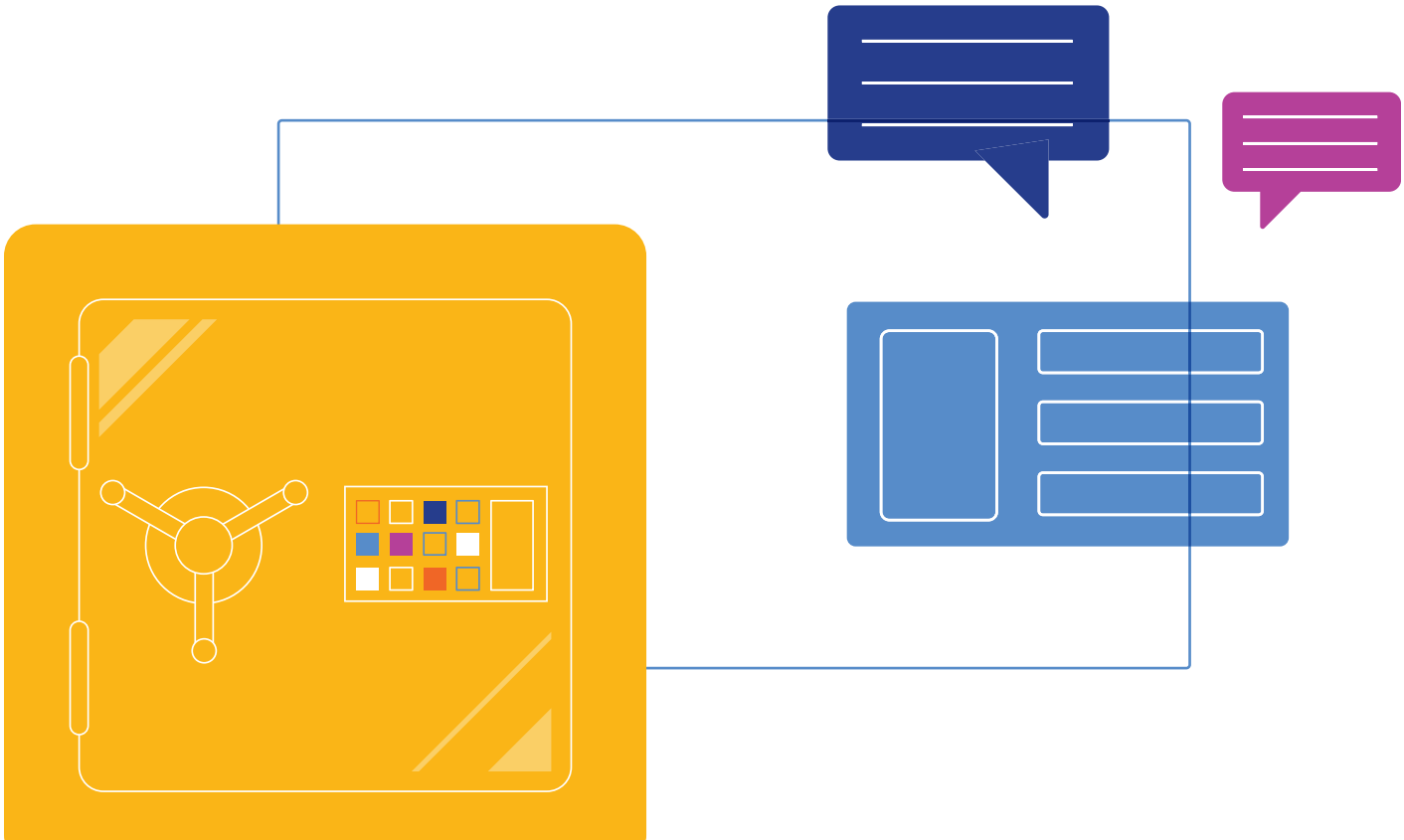
Questions that are maintained by a group of companies to help evaluate a vendor's security and privacy.

Higher Education Community Vendor Assessment Tool (HECVAT)

Questionnaire to help higher education institutions assess vendor risk.

NIST standard 800-171

Recommendations for protecting controlled unclassified information.



Security Definitions

Antivirus/Anti-Malware

Prevents, detects, and removes malicious software from the systems they run on.

Disaster Recovery Plan

A formal plan to resume normal operations after a disaster (weather events, equipment damage, etc.) that disrupts and impacts business activities.

Incident Response Plan

A plan with procedures in response to a data breach as it occurs to help contain and remove the threat.

Intrusion Detection System (IDS) and Intrusion Protection System (IPS)

Monitors network traffic and alerts to a threat. An IPS takes action to block or remediate identified threats in network packets.

Logging tools

Allows organizations to discover nefarious activities before they spread to other systems and gives insight into what the attacker did or tried to do which helps with efficient remediation.

Multifactor Authentication (MFA)

Ensures user identity by requiring that they provide at least two pieces of evidence to prove their identity. Each piece of evidence must come from a different category: something they know, something they have, or something they are. MFA should be implemented wherever possible.

Next Generation Antivirus

System-centric, cloud-based approach that uses predictive analytics driven by machine learning and artificial intelligence which combines with threat intelligence.

Recovery Time Objective (RTO)

The agreed-upon *quantity of time* that an application, system and/or process, can be down for without causing significant damage to the business as well as the time spent restoring the application and its data.

Recovery Point Objective (RPO)

The *amount of data* that can be lost within a period before significant harm occurs from the point of a critical event to the recent backup.

Single sign-on (SSO)

Provides a source of truth for any integrated solution that allows for the centralized management of identity and authentication. Only requires one password/login to access different tools.

Honorlock Security

At Honorlock, security is a foundational element of everything we do.

We never sell or monetize your data with third-parties

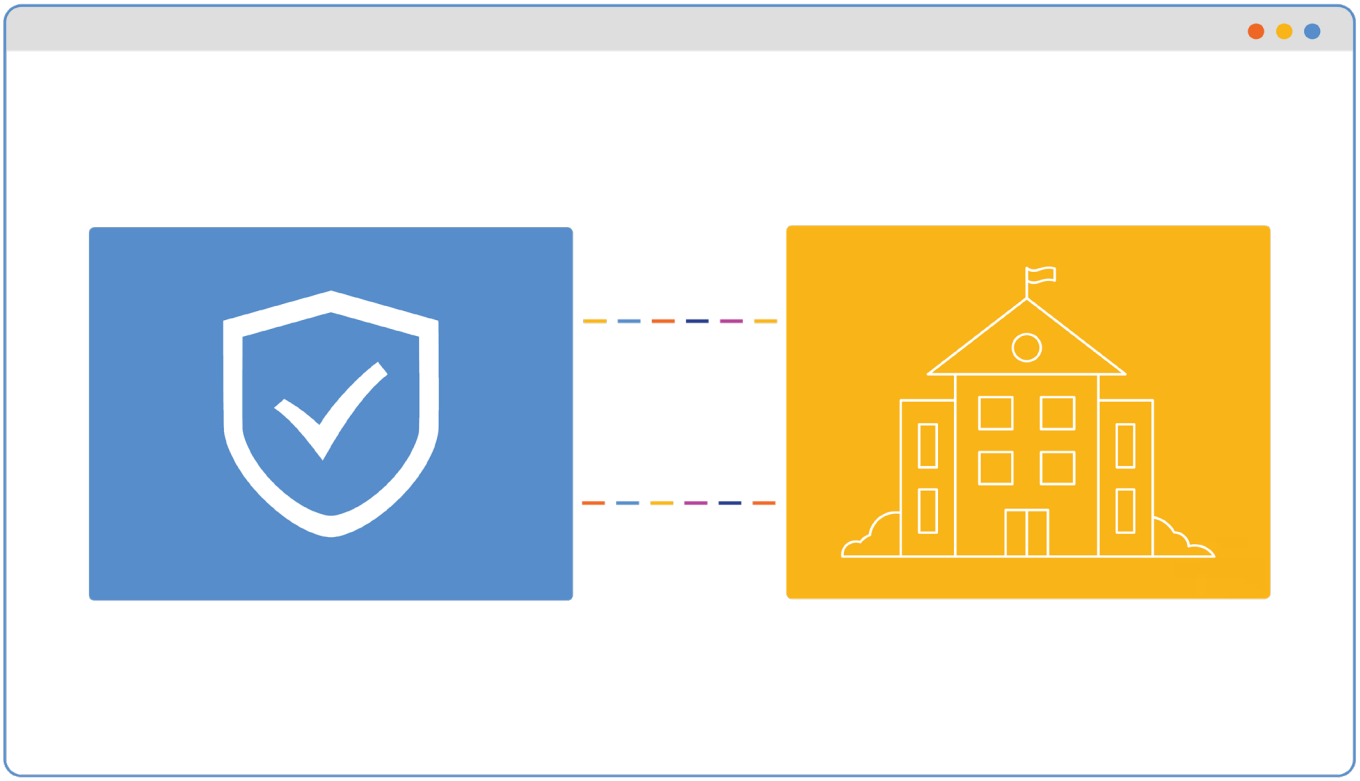
Honorlock maintains a public-facing privacy policy that clearly states that we will never sell or monetize your data with third parties.

Your institution owns the data

The institution owns the data and retention is governed by the MSA.

Your data is encrypted in both storage and at rest

Honorlock utilizes Amazon Web Services for our secure hosting needs. Amazon's data centers are SOC 3 certified and exercise some of the most stringent physical security in the industry.



Employee onboarding

Before joining the organization every new employee receives a background check and signs a Non-disclosure agreement.

As part of onboarding, each employee undergoes security training that covers compliance, information security, data classification, data handling, reporting security incidents, and much more.

Ongoing security training for employees

Honorlock conducts annual security and privacy training for employees because it isn't enough to put people in a training room once a year and go through a 30-minute PowerPoint.

We employ proactive security testing that simulates attacks against our most valuable defense - our people.

At Honorlock, we challenge everyone to think about how their actions will affect the data we are entrusted with.

We treat your data like we would want our data to be treated.

Vendor RIsk Assessment

Before onboarding a new vendor or sub-service organization that has access to confidential data, Honorlock performs a vendor assessment to ensure that each vendor passes our security, data, and privacy requirements.

Disaster recovery to prepare for the unexpected

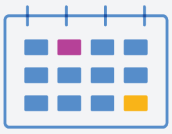
We have Disaster Recovery & Business Continuity Plans that we test at least annually. We also operate our infrastructure in multiple availability zones which increases our resiliency to downtime.

Honorlock Online Proctoring

Simple, Secure, and Scalable Online Proctoring

Honorlock combines AI & live test proctors to make online proctoring simple, easy, and human.

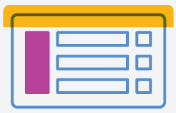
Online proctoring features as unique as your exams



No Exam Scheduling

Human Proctors & AI Proctoring Software

Detect Cell Phones



Proctor Third-Party Exams

Fast Student ID Verification

Search for Illicit Exam Content

To learn more, visit honorlock.com