# HDI Security Protocols Ensure Data is Kept Private

When it comes to data security, we are all working toward the same goal of achieving reliable protection. HDI Solutions, LLC has never experienced a data breach because we stick to tried-and-true industry standards and mainstream best practices that are proven to protect sensitive client data.

The flow of information is constant in today's world, and for a business to be successful it likely needs to have a solid, secure online presence. However, the digital world brings vulnerabilities and security threats that can set government agencies, private companies and their stakeholders or customers back if not managed properly.

**Consequences of a Data Breach**
Unfortunately, data breaches take place daily and can wreak havoc on a system and its users. In addition to causing physical damages, a breach in security can also injure an agency or company's reputation with its constituents or customers.

Any time a customer's personal information is accessed or used without consent due to a security breach, the organization takes a hit when it comes to credibility and trust in the public eye. When a government agency or private company works with HDI to develop a system that incorporates proper security protocols, they can ensure their customers that their data is in trustworthy and protective hands.

## High Security Standards

**Open Web Application Security Project (OWASP)**
When it comes to security, our team starts with the basics. HDI follows OWASP – Open Web Application Security Project – standards to identify vulnerable areas of software development which lend themselves to malicious attacks.

OWASP provides an ongoing list of top areas of exploit within software security and offers strategies for how to prevent and address those potential weaknesses. HDI uses OWASP's standards to guide the development process and ensure proper security protocols are put in place for each client's system.

The OWASP Top Ten Vulnerabilities are outlined below:

- Injection – the attempt to trick systems into executing commands to access data without proper authorization
- Broken Authentication – allowing hackers to compromise passwords or other sensitive system access credentials or even hijack user credentials
- Sensitive Data Exposure – the compromise of weakly protected data which leaves client data open to fraudulent activities
- XML External Entities – external actors gaining system access for activities such as internal port scanning and denial of service attacks
- Broken Access Control – exploiting system vulnerabilities to view sensitive system information, modify data or alter system access rights
- Security Misconfiguration – one of the most common vulnerabilities, hackers can exploit poor security configurations to access systems and data
- Cross-Site Scripting XSS – this vulnerability allows bad actors to execute scripts which can result in activities such as overtaking user sessions or directing users to malicious sites
- Insecure Deserialization – this vulnerability can allow for remote code executions and attacks including injection and privilege escalation attacks.
- Using Components with Known Vulnerabilities – the exploitation of known vulnerabilities by attackers can lead to complete server takeovers and severe data loss
- Insufficient Logging and Monitoring – systems

# HDI Security Protocols Ensure Data is Kept Private


with insufficient logging and monitoring services can allow attackers free reign over systems. Many breach studies show that it can take more than 200 days to detect a breach if internal logging and monitoring are not in place and continuously reviewed

## Addressing Security Across a System

**Standard Company Policies**
We approach each project, no matter the client, using standard protocols and considering the following:

- Access controls
- Training and awareness
- Audit and accountability
- Security assessments
- Configuration management
- Contingency planning
- Authentication and authorization
- Appropriate use; incident response; risk assessment; systems development; data protection

Some clients, depending on the system being developed, may need to focus on one area more heavily than others. Because HDI builds custom system solutions we have the flexibility to meet any security requirements needed, but a solid security foundation is set for every client.

**In-App Security Foundation**
Based on OWASP standards, as the HDI team goes through the development process, we consider all vulnerabilities and implement safeguards to protect the system from potential threats. HDI emphasizes the need to build the system with strong security protocols from the ground up – that way, if someone were to break through the outer layers of security, there are still safeguards in place within the application to limit potential damage.

**Encryption for the Transportation and Storage of Data**
When it comes to transport and storage of information, HDI uses AES-256 encryption software, which is the most commonly accepted level of encryption. If data is resting in a database it is encrypted, and if it is being moved from server to users, HDI uses TLS (Transport Layer Security) certificates to encrypt the information as it is in transit.

**User Role Security and Limited System Access Points**
Typically, the systems we develop are limited in the number of access points available. We build user role-based security within the application, so based on a person's role in the company or their use of the application, we limit what they can do based on the needs of their authorized use of the resulting system. This requires at least one level of authentication (sometimes dual authentication) to limit access of others.

By doing this, we can use our firewall to only allow people who are designated into the system. For example, if you were working from home and connected to your organization through a VPN, you would still be able to access the system through your organization's IP address being whitelisted. On the other side, if an outside source was to try to hack into the system but were not on the authorized user list, they would be unable to access the VPN.

Limiting system access points is especially important to secure systems that involve collection or storage of personally identifiable information (PII). PII could include names, health records, social security numbers, driver's license numbers and other sensitive data.

Any time a government agency or private company

# HDI Security Protocols Ensure Data is Kept Private

uses software with this type of personal data, there is a need to go above and beyond to keep that data secure within the system and protect the system from potentially threatening outside access. Take fraudulent unemployment claims as an example. Someone would have to get into a database for names and addresses, but if they are successful, they can immediately use that information to try and claim unemployment. All they need are a name and address and can instantly cause a host of issues for the system operator and its customers.

**Firewall Monitoring 24/7**
HDI contracts with a third party, SecureWorks, to monitor the firewall 24 hours a day, 7 days a week. SecureWorks uses a sophisticated monitoring algorithm that can detect suspicious activity at the firewall, and alert HDI and/or the client if there are issues. If there is a threat, it can be shut down before any damage is caused.

This extra layer of security keeps threats at arm's length and operates in addition to the safeguards mentioned previously within the system.

*Security Protocols*
Under the direction of HDI's Information Systems Security Officer, HDI constantly scrutinizes its own security policies to ensure all standards are met, policy updates are implemented, and new technologies are utilized. HDI's ISO maintains active CISSP, CISA, CRISC and CDPSE certifications and has a research focus in inter-organizational use of cloud-based information technologies, which has been of paramount importance as more systems migrate to the cloud.

Thanks to our work with both government agencies and private companies, HDI develops systems that are compliant with state and federal standards when it comes to security:

- NIST
- FIPS
- CJIS
- HIPAA
- OWASP
- TLS
- PGP Encryption
- Sophos Anti Virus Protection
- SonicWall Firewall Management

HDI can customize system security protocols based on the data being collected, including PII. We treat all data as if it's highly sensitive, which is why we've never experienced a data breach during our company history.

## Trust HDI with Your System, and Your Customers Will Trust You

We handle security protocols the right way, following industry standards and mainstream solutions with a goal to keep client data fully protected at all times. HDI uses industry standard programming languages, databases, storage environments and other tools to ensure our system security is reliable and consistent.

HDI can help you balance the need to meet consumers where they are – online – with keeping their data private and secure.