

# Choose a Secure Information Management Solution

Use these questions to guide your security discussion with potential vendors



The right information management solution will help secure your valuable business and customer data. Your new solution should reduce risk and improve regulatory compliance rather than introduce new risks and vulnerabilities into your organization. This worksheet will help you examine potential solutions against security requirements.

## SECURITY PROTOCOLS DURING PRODUCT DEVELOPMENT

	Hyland	( Vendor 2 )	( Vendor 3 )
<b>DOES THE VENDOR:</b>			
Take security into consideration at every phase of the product lifecycle?	✓		
Have a dedicated security team?	✓		
Utilize development staff trained in secure development practices?	✓		
Use secure development practices in every step of the development and design process?	✓		

**OnBase by Hyland:** Hyland considers application security in every step of product development. Built-in “gates” require the security team to sign-off on development before the next phase can begin.

VENDOR 2: NOTES

VENDOR 3: NOTES

## CUSTOMER OFFERINGS AND TRAINING

	Hyland	( Vendor 2 )	( Vendor 3 )
<b>DOES THE VENDOR:</b>			
Offer free upgrades to the latest, most secure version of their software?	✓		
Provide any product-specific security training courses for system admins or software end users?	✓		
Prepare the product for compatibility with new infrastructure versions or patches (i.e. Windows patches, new browser versions, etc.)?	✓		

**OnBase by Hyland:** Our security team provides training to the entire R&D staff – including both developers, testers and customers. Their security expertise and consultation is leveraged throughout the entire company.

VENDOR 2: NOTES

VENDOR 3: NOTES

## PROTECTION IN EVERY DATA STATE (AT REST, IN TRANSIT, IN USE)

	Hyland	( Vendor 2 )	( Vendor 3 )
<b>DOES THE VENDOR'S PRODUCT:</b>			
Provide the ability to prevent unauthorized parties – internal and external – from viewing sensitive data if the database is accessed?	✓		
Use end-to-end encryption (via HTTPS/TLS) to protect data in transit?	✓		
Offer the ability to hide sensitive data values while in use?	✓		
Work in conjunction with infrastructure security features, including TLS, full disk encryption and antivirus?	✓		
Salt and hash passwords using a secure hash algorithm (i.e. PBKDF2) before being stored in the database?	✓		

**OnBase by Hyland:** All data stored in OnBase can be encrypted with AES-256 or AES-128. TLS is supported to protect communication of data end to end. Configurable session timeouts and keyword masking prevent unauthorized users from active user devices.

VENDOR 2: NOTES

VENDOR 3: NOTES

## DEFENSES AGAINST THIRD-PARTY VULNERABILITIES AND NEWLY DISCOVERED ATTACK VECTORS

	Hyland	( Vendor 2 )	( Vendor 3 )
<b>DOES THE VENDOR:</b>			
Test for common vulnerabilities such as those listed in the OWASP Top 10?	✓		
Have software developers and QA staff trained in penetration testing techniques and in preventing common security vulnerabilities?	✓		
Quickly alert customers to any vulnerabilities in their product?	✓		
Follow protocols to ensure their product is safe against newly-discovered attack vectors?	✓		
Consistently test to identify whether or not their product is impacted by third-party vulnerabilities?	✓		
Use a third-party security firm for active penetration testing?	✓		

**OnBase by Hyland:** At Hyland, we continuously test for vulnerabilities, exploits, vectors and bugs, including: Secure development practices, automated security scanning and manual penetration testing.

VENDOR 2: NOTES

VENDOR 3: NOTES

## EASE OF CONFIGURATION

	Hyland	( Vendor 2 )	( Vendor 3 )
<b>DOES THE VENDOR'S PRODUCT:</b>			
Provide out-of-the-box security defaults?	✓		
Pre-configure safeguards against security misconfiguration?	✓		
Require specialized OnBase personnel for deployment?	✓		
Make secure deployment and infrastructure best practice documents readily available?	✓		
Offer the ability to configure user group rights and role-based access to protect data from unauthorized access?	✓		
Allow for the segregation of data based on a metadata value without special coding?	✓		
Enable the rotation of encryption keys in the event of a breach without using specialized code?	✓		

**OnBase by Hyland:** Security functionality comes standard with OnBase. These access controls include strict policies with configurable complexity requirements as well as granular rights management that enables admins to control access to every part of the system.

VENDOR 2: NOTES

VENDOR 3: NOTES

Hyland	( Vendor 2 )	( Vendor 3 )
Final Remarks:	Final Remarks:	Final Remarks:

For more tips on securing your information management solution, [visit onbase.com/security](https://onbase.com/security).