Vound's Security Assessment Response

Vound's responses to Security Assessment Questionnaires

The answers provided are based on findings from an ISO Compliance audit conducted by an independent third-party certifier. As the detailed findings from this audit constitute intellectual property, Vound is unable to disclose any additional information beyond what is provided here. While these responses may not align precisely with the format or specific questions requested by your organization, they address a broad range of commonly asked security-related inquiries.

Please note that Vound is unable to provide this information in any other format or respond to alternative variations of these types of questions.

Also attached is
our ISO 27001 certificate. Link to certification record: https://www.iafcertsearch.org/certification/F2W9lyb161Lrl15q6Hx3BsgS
Please note this is the maximum we will supply on our security posture.

#	Item	Response	Additional Information
	Policies and Procedures		
	Is a senior official/officer within your company directly responsible for the oversight and implementation of the security policies at your company?	Yes	
	Are procedures employed throughout your company to ensure compliance with privacy laws/regulation requirements related to maintaining security, confidentiality and protection of third party personal information (i.e., information pertaining to your customers' employees, customers and/or producers)?	Yes	
	Has your customer data ever been breached? If yes, please explain the extent of the breach and the controls you implemented to prevent future breaches.	No	
	Do you have a breach response plan?	Yes	
	Are your security policy document(s) published and enforced in your organization?	Yes	
	Are these procedures communicated to your subcontractors who may have access to customer data?	Yes	
	Are these procedures being monitored?	Yes	
	Are policies and procedures updated frequently?	Yes	
	Do you have staff assigned to the following:		
	Security Awareness?	Yes	
	Policy Enforcement?	Yes	
	Risk Evaluation?	Yes	
	Risk Mitigation?	Yes	
	Regulatory Compliance?	Yes	
	Do you have policies and procedures covering the following:		
	HR Practices?	Yes	
	Authorized/acceptable use of Networked Services?	Yes	
	Use of Corporate Email, intranet and Internet?	Yes	
	Password Management?	Yes	

	Software/Hardware Acquisition?	Yes	
	Change Management?	Yes	
	Encryption Policy and Standards?	Yes	
	Security related incidence response/handling?	Yes	
	Data Handling Policy (to include data use, storage and destruction of sensitive data)?	Yes	
	Third Party Access & Remote Access?	Yes	
	Do you outsource any security management functionality? *If yes, please explain.*	Yes	Cybersecurity consulting - compliance, pen testing, vuln scans
	Are the consequences of non-compliance to the policies clearly documented?	Yes	

	Background Checks		
	Do you perform background checks on your employees?	Yes	Where legal to do so.
	2 full reference verifications?	Yes	
	5 year county criminal check?	Yes	
	Social security number verification?	Yes	
	Do you perform background checks on your contractors?	Yes	Where legal to do so.
	2 full reference verifications?	Yes	
	5 year county criminal check?	Yes	
	Social security number verification?	Yes	

	Physical Security		
	Which of the following physical security/perimeter control(s) do you have at your facility(ies):		
	Security Guards?	No	
	Security Cameras?	Yes	
	Employee Identification Cards or Badges?	Yes	
	Visitor Identification Cards or Badges?	Yes	
	Locked storage areas to store customer personal information?	N/A	Customer Data of any kind is not stored, accessed, or transmitted by Vound.
	Do you monitor and escort visitors through sections of your facilities?	Yes	
	Do you maintain visitor logs for more than 30 days?	Yes	

	Disaster Recovery and Business Continuity		
	Do you have a Disaster Recovery and/or Business Continuity Plan?		Yes
	Do you test your recovery plans? If so, How often?	Yes	Annually or upon material change to the plan or the organization.
	What type of testing do you conduct (i.e. paper walkthrough or simulation drills)? *Please respond in comments field.*		scenario based live tabletop exercise and simulation
	Are the recovery procedures tested for efficacy?	Yes	
	Are manual backup/restore procedures documented and practiced in case of automatic backup failure?	Yes	
	Will we be permitted to participate or review your test to ensure we can establish connectivity and access systems at the recovery site?		No. A virtual site walkthrough was performed by an independent third party ISO assessor as part of their testing procedures.
	How long do you estimate it will take to restore product or services should you experience a serious business interruption (interruption that lasts more than 1 business day) *Please respond in comments field.*		< 4 hrs

	Can you meet recovery time objective(s) (RTO) and recovery point objective(s) (RPO) for all products and services contracted with us?	Yes	
	Is this estimate based on previous test results of the recovery plans?	Yes	
	Do you have pre-arranged recovery locations? *If so, where are they?*	Yes	geographically segregated zones
	Physical and Information Security		
	Do you have a data center at this location?	No	
	Do you have the following perimeter control(s) applied to data center?		
	Tokens/Cards?	N/A	No data center
	Key Pad Controls?	N/A	
	Man Trap?	N/A	
	Biometric Controls?	N/A	
	Guards?	N/A	
	Do you monitor/log all access to data center?	N/A	
	Do you have redundant public utilities connections?	N/A	
	Do you employ UPS (Uninterrupted Power Supply), Battery Banks, Generators etc?	N/A	
	Do you employ fire/flood detection and suppression systems?	N/A	
	Can you provide a recent SOC-2 report, ISO 27001 report or other industry recognized audit report?	Yes	Vound will only supply the ISO certificate and not the details of the ISO.
	Do you limit administrator level access on network and systems infrastructure to system administrators only?	Yes	
	Is access to security logs strictly controlled (Firewall logs, etc.)?	Yes	
	Do you employ version management, build & deploy process?	Yes	
	Do you have policies in place preventing your employees from copying our data to mobile devices, external media or forwarding it to third party e-mail?	Yes	
	Do you have Data Loss Prevention tools in place to enforce the policy above?	Yes	
	Accounts Management & Access Control		
	How will our data be secured at your site?	N/A	Customer Data of any kind is not stored, accessed, or transmitted by Vound.
	Who will have access to our data?	N/A	Customer Data of any kind is not stored, accessed, or transmitted by Vound.
	How do you prevent other clients from accessing our data? *Please respond in comments field.*	N/A	Customer Data of any kind is not stored, accessed, or transmitted by Vound.
	How and where are user IDs and Passwords stored? How are they secured and what type of encryption is used?	N/A	Customer Data of any kind is not stored, accessed, or transmitted by Vound.
	Will the access credentials be encrypted when passing through public networks? *Please describe encryption type in comments field.*	N/A	Customer Data of any kind is not stored, accessed, or transmitted by Vound.
	Do you employ any mechanisms that facilitate secure data exchange such as SSL, FTP, etc?	N/A	Customer Data of any kind is not stored, accessed, or transmitted by Vound.
	E-Commerce (applicable if vendor does business on-line)		
	Are the following maintained in e-commerce system:		

	Confidentiality?	Yes	
	Authorization?	Yes	
	Non-Repudiation?	Yes	
	Transaction Integrity?	Yes	
	Access codes encrypted in storage and transmission?	Yes	

	Patch Management		
	Do you apply security patches on a regular basis?	Yes	
	Do you have an automated patch management solution deployed? *If no, please explain.*	Yes	
	Are software patches reviewed, tested, and applied on a timely basis?	Yes	

	Network Infrastructure		
	Do you maintain up-to-date network infrastructure and administration procedures?	Yes	
	Do you have perimeter scanning/monitoring agreements with managed network services providers?	Yes	
	Are all your routers configured with access control lists to allow only specific traffic to pass through?	Yes	
	Do you allow access to your routers via its console port or a secured connection?	Yes	
	Are all your networking devices at the latest patch level? *If no, please explain.*	Yes	
	Do you have a procedure to keep track of announcement of vulnerability patches for your networking devices?	Yes	
	Do you ensure default passwords are changed on networking devices?	Yes	
	Do you control the change frequency and distribution of admin access to network infrastructure?	Yes	
	Do you use 802.1x complaint security for your wireless network? *If yes, what vendor and type (e.g. none, WPA, WPA2)?*	Yes	
	Do you monitor the security/policy violations and application/networked services availability?	Yes	
	Do you log successes and failures to access? If yes, is there a process in place to review the log and address anomalies?	Yes	
	Do you do penetration testing. If so please supply the most recent vulnerabilities scan result (Pentest report or its executive summary preferred).	Yes	Vound will only supply the ISO certificate and not the details of the or testing that was undertaken as part of the ISO audit.

	Remote Access and VPN		
	Are there any remote access/remote control methods available to access your network, as follows:		
	RADIUS?	No	
	User ID/Password?	Yes	
	Token based access control?	No	
	Do you allow supervisory/admin functions to be performed over unencrypted external links? *If yes, please explain.*	No	
	Do you collect/review audit log data on remote access?	Yes	

	Firewall		
	Do you employ Firewall(s) to protect your network?	Yes	
	Do you have any other applications (e.g. DNS, DHCP) running on the same Firewall? *If yes, please explain.*	No	
	Are your Firewall's Operating system & software at the latest patch level? *If no, please explain.*	Yes	
	Do you allow non-standard (>1024) IP ports passing through your Firewall? *If yes, please explain.*	No	
	Do you regularly scan and verify all the allowable services provided by your Firewall?	Yes	
	Do you use firewall-reporting tools to analyze your Firewall log?	Yes	
	Do you have your security policy on your firewall documented, verified and reviewed periodically?	Yes	
	Do you protect your internal IP address range(s) (e.g., use NAT/RFC 1918)?	Yes	

	Malware Controls		
	Do you scan all emails for viruses?	Yes	
	Is there explicit policy requiring anti-virus software on networked computers?	Yes	
	Do you have centralized administration of virus control, such as distribution of signature updates, reporting, policy enforcement and vendor management?	Yes	
	Are rules established for scanning outside software?	Yes	
	Does the virus checking software run in the background with established frequency of scanning, etc.?	Yes	
	Are end-users prevented from disabling anti-virus software on personal computers?	N/A	Personal computers are not in use, only Vound corporate assets.
	Do you allow installation of personal and non-corporate approved software or hardware on network computers? *If yes, please explain.*	No	

#	Software Development Practices		
	Is the software developed and built in secure environments.	Yes	
	Are those environments secured by the following actions, at a minimum:	Yes	
	Separating and protecting each environment involved in developing and building software;	Yes	
	Is Regularly logging, monitoring, and auditing trust relationships used for authorization and access: i) to any software development and build environments; and ii) among components within each environment;	Yes	
	Is enforcing multi-factor authentication and conditional access across the environments relevant to developing and building software in a manner that minimizes security risk;	Yes	
	Do you take consistent and reasonable steps to document, as well as minimize use or inclusion of software products that create undue risk within the environments used to develop and build software;	Yes	
	Do you encrypt sensitive data, such as credentials, to the extent practicable and based on risk;	Yes	
	Do you use defensive cybersecurity practices, including continuous monitoring of operations and alerts and, as necessary, responding to suspected and confirmed cyber incidents;	Yes	

	Do you make a good-faith effort to maintain trusted source code supply chains by employing automated tools or comparable processes to address the security of internal code and third-party components and manage related vulnerabilities;	Yes	
	Do you maintain provenance for internal code and third-party components incorporated into the software to the greatest extent feasible;	Yes	
	Do you employ automated tools or comparable processes that check for security vulnerabilities. In addition:	Yes	
	Do you undertake these processes on an ongoing basis and prior to product, version, or update releases;	Yes	
	Do you have a policy or process to address discovered security vulnerabilities prior to product release	Yes	
	Do you have a vulnerability disclosure program and accepts, reviews, and addresses disclosed software vulnerabilities in a timely fashion and according to any timelines specified in the vulnerability disclosure program or applicable policies.	Yes	

Certificate Number:
IA-2025-02-18-01

Date of Initial Issue:
February 18, 2025

Date of Issue:
February 18, 2025

Certificate Version:
V1.0

Expiration Date:
February 18, 2028

SoA Version:
V1.2

SoA Date:
November 11, 2024

Insight Assurance
IAS ACCREDITED
MSCB-306

Certificate Of Registration

This is to certify that the Information Security Management System of:

Vound Colorado Ltd

Address: 10643 N Frank Lloyd Wright Blvd Scottsdale AZ 85259

has been assessed by Insight Assurance and found to be in conformance to the following standard:

ISO/IEC 27001:2022

The scope of the certification is the Information Security Management System (ISMS) supporting the Intella software product. The ISMS includes all personnel, assets, and information necessary to support the ISMS. Functional areas that support the ISMS are IT, Client Services, Operations, HR, and Information Security.

Felipe Saboya
Partner I CPA, CIS LA

Jesus Jimenez
Partner I CISA, CIS LA, CIS LI, QSA, CDPSE

Certificate Number:
IA-2025-02-18-01

Date of Initial Issue:
February 18, 2025

Date of Issue:
February 18, 2025

Certificate Version:
V1.0

Expiration Date:
February 18, 2028

SoA Version:
V1.2

SoA Date:
February 11, 2024

Insight Assurance
IAS ACCREDITED
MSCB-306

Certificate Of Registration

Site	Activities / Sub-scope
10643 N Frank Lloyd Wright Blvd Scottsdale AZ 85259	IT, Client Services, HR, Information Security