Server & Security Information Kit

Server Configuration

Montoring Rules

Infrastructure

Monitored Metrics	Alert Conidition	Alert Timeout	Alert Iteration
VM Availability	Down	5 Min	2 Hr
memory usage	< 5% left	5 Min	2 Hr
Unusual network throughput in	> 100 MB/s	5 Min	2 Hr
Unusual network throughput out	> 100 MB/s	5 Min	2 Hr
Out of disk space	< 10% left	5 Min	2 Hr
High CPU load	> 90%	5 Min	2 Hr
Swap is filling up	> 90%	5 Min	2 Hr
Physical component too hot	temp_celsius > 75	5 Min	2 Hr
Physical node temperature alarm	1	5 Min	2 Hr
Unusual disk read rate	> 50 MB/s	5 Min	2 Hr
Unusual disk write rate	> 50 MB/s	5 Min	2 Hr
Disk will fill in 4 hours	current write rate	5 Min	2 Hr
Unusual disk read latency	read operations > 100ms	5 Min	2 Hr
SystemD service crashed	state="failed"	5 Min	2 Hr
Zombie process	> 50	5 Min	2 Hr
SSH Sessions	> 10	5 Min	2 Hr

Services

MySQL

Services Availability	MySQL down	5 Min	2 Hr
MySQL too many connections	> 80%	5 Min	2 Hr
MySQL high threads	> 60%	5 Min	2 Hr
MySQL slow queries	> 0	5 Min	2 Hr
MySQL restarted	uptime < 60	5 Min	2 Hr

Montoring Rules

Services

Apache

website and SSL

Monitored Metrics	Alert Conidition	Alert Timeout	Alert Iteration
Services Availability	Apache down	5 Min	2 Hr
Apache workers load	> 80%	5 Min	2 Hr
ApacheRestart	uptime < 60	5 Min	2 Hr
SSL certificate will expire soon	< 7 days	5 Min	2 Hr
SSL certificate expired	0 days	5 Min	2 Hr
The website doesn't response	0	5 Min	2 Hr
Slow response	> 2 seconds	5 Min	2 Hr
HTTP status code is not 200-399	>= 400	5 Min	2 Hr
HTTP request took more than 1s	>1	5 Min	2 Hr
Slow ping (High Latency)	>1	5 Min	2 Hr

Backup

Internal

Backup Location	Backup Type	TIme	Retention
locally	Compressed	Every Day at 2 AM	1
locally	Compressed	Evey Starday at 2 AM	1
locally	Compressed	1st day of the month at 2 AM	1

External

Acronis Cloud Backup	Compressed	Weekly at 2 AM	15

Firewall

Firewall Type	Software
AWS Secuirty Group	AWS Secuirty Group
Internal Software Firewall	CSF

Zone1 servers run on Amazon Cloud/ Amazon Web Services (AWS)

Computer Security Incident Response Procedure

1. Purpose

The purpose of this procedure is to provide instructions on security incident response to the management, employees, and contractors of Zone1.

2. Definitions

A security incident response incident includes but not limited to:

- A malware outbreak affecting one or more computers that can pose a serious harm to the confidentiality, integrity, and availability of Zone1 systems or information.
- A Distributed Denial of Service (DDoS), a form of electronic attack involving multiple computers, which send repeated requests or pings to a server(s) to overload the system and render it inaccessible for a period of time.
- A suspected privacy or security breach that impacts the confidentiality or integrity of Zone1 data.
- A website defacement.
- A theft by an employee of production data.
- An inadvertent loss of data due to human error.
- Customer notification that Zone1 data has been release in an unauthorized manner.
- Observation of Zone1 data being shared in an unauthorized manner on the internet on sites.
- Unknown or unexpected outgoing Internet network traffic from the production environment that houses PHI.
- Unexplained modification or deletion of data.
- Anti-virus programs malfunctioning or becoming disabled for unknown reasons.
- Excessive failed login attempts in system authentication and event logs.
- Vendor or third-party connections made to the production environment without prior consent and/or a trouble ticket.
- Authentication event log modifications (i.e., unexplained event logs are being deleted).
- Suspicious after-hours file system activity (i.e., user login or after-hours activity).
- Unexplained new user accounts.
- Variances in log chronology or timestamps.

3. Scope

This procedure applies to all employees, contractors, and third-party service providers of Zone1.
Applicable provisions of this policy must be addressed in Zone1's agreements with third party service providers as required.
This policy applies to Zone1's services which may impact the privacy or security of clients' data in Zone1's care.

4. Roles and Responsibilities

1. **Staff and Service Providers** of Zone1 are responsible for reporting privacy incidents or breaches to its clients within a reasonable time and for cooperating with any investigation of an incident or breach.

2. **Information Technology and DevOps (IT):**
Information Technology plays the role of security expert with necessary training to be able to identify which events contribute to an incident and which are false positives. Often but not always, IT personnel will have formalized training to maintain these skills. IT is formally assigned the responsibility for monitoring and analyzing security alerts and reporting it to the Managing Director.

3. **External Vendors**
External Vendors provide some form of service to Zone1 and are required to react based on instructions that CSIRT provides in a timely manner. An example of an External Vendor is AWS.

4. **Computer** Security Incident Response Procedure

5.1 **Overview**

A security incident response capability will be developed and implemented for all information systems that house or access Zone1 controlled information. The incident response capability will include a defined plan and will address the seven stages of incident response:

a. Preparation
b. Detection
c. Analysis
d. Containment
e. Eradication
f. Recovery/Fortification
g. Post-Incident Activity

To facilitate incident response operations, responsibility for incident handling operations will be assigned to the IT team. If an incident occurs, the members of this team will be charged with executing this incident response plan.

Incident response will be tested at least annually using tabletop exercises. Where appropriate, tests will be integrated with testing of related plans such as the Business Continuity Plan or Disaster Recovery Plan. The results of these tests will be documented and shared with key stakeholders.

Incident response plans will be reviewed and, where applicable, revised as circumstances or environments change within Zone1. Review will be based upon the documented results of previously conducted tests or live executions of the incident response plan. Upon completion of plan revision, updated plans will be distributed to key stakeholders.

5.2 **Preparation**

Zone1 must conduct a tabletop exercise once per year to ensure the members of the IT team are aware of their roles and responsibilities and to use the testing as a means of testing the effectiveness of the plan and adjust were required.

5.3 **Detection & Analysis**

This phase deals with the detection and analysis of incidents within the Zone1 environment are true or false positive security incidents. Confidentiality, Integrity and Availability (CIA) or Zone1 systems are used to help categorize the potential incident.

Sample Cyber Incident	CIA Category	Privileged Account Breach	Business Impact	Risk Level
An employee shares information with an unauthorized third party, but the information is not personal or protected by regulatory requirements.	C	No	Low	Low
Malware hidden within a program leverages local credentials to execute but doesn't access privileges of a DevOps Engineer. Adware appears on the employee's computer.	C, I	Yes	Low	Low
A cyber-criminal uses a pass-the-hash technique to steal passwords and access multiple databases and root accounts.	C	Yes	High	High
The cyber-criminal uses privileged access to overwhelm the system with requests, slowing performance and damaging the user experience.	C, I, A	Yes	High	High
A malware outbreak is detected on multiple computers or servers.	C, I, A	Potential	High	High
DDoS is detected due to client facing portals being unavailable and this is confirmed within the traffic logs.	A	No	High	High
DoS is detected due to slow or unresponsive servers and investigated.	A	No	High	High
Unauthorized Data Exfiltration.	C	Potential	High	High
Website Defacement.	I	No	High	High
Employee Theft of Data.	C	Potential	High	Medium
Inadvertent Data Loss.	C	No	High	Low
Variances in log chronology or timestamps.	None	No	Low	Medium

Zone1 will implement measures to detect privacy and security incidents, including:

1. Monitoring and audit of user access by Zone1 personnel including employees, contractors, and other authorized agents.
2. Monitoring and audit of access or attempted access by external malicious agents.
3. Receiving complaints from individuals or their authorized representatives that might indicate that a breach has occurred.
4. Receiving notice from 3rd party suppliers that a breach or suspected breach has occurred at the supplier's site.
5. Responding to privacy breach investigations initiated by Clients.
6. Responding to privacy breach investigations initiated by an Information and Privacy Commissioner (IPC) or regulator.

5.4 **Containment**

Immediately upon determining that a privacy or security incident has occurred, Zone1 will take measures to contain the incident. Measures may include, but not limited to:

1. Suspending access to users who may have been party to the incident.
2. Requiring authorized users to change their passwords.
3. Temporarily shutting down the system, if needed.
4. Contacting the police if the breach involves theft or other criminal activity.
5. Immediately upon determining that a privacy or security incident has occurred, Zone1 will secure all audit logs and any other evidence associated with the incident.
6. Immediately upon determining that a privacy or security breach has occurred, Zone1 shall take measures to mitigate any harm to individuals because of the incident.

5.5 **Notification**

Where it is determined that a breach of data has occurred:

1. Zone1 will notify every applicable client at the first reasonable opportunity that there has been a breach of the data.
2. Clients are responsible for notifying individuals (i.e. substitute decision makers) at the first reasonable opportunity if their data is stolen, lost, or accessed by unauthorized persons.
3. Zone1 will provide assistance to clients to enable them to identify, contact and inform individuals affected by the breach. Individuals may be informed about the circumstances of the breach, what information was used or disclosed, measures taken to mitigate any harm resulting from the breach, and advice to individuals about measures they can take to further mitigate any potential harm.

5.6 **Investigation and Remediation**

1) Once a privacy or security incident or breach has been appropriately contained, it shall be investigated by the IT team. The investigation will identify the root cause of the incident or breach as well as the information assets, individual(s)/organization(s), and IT systems and hardware involved in the incident or breach.

Evidence will be collected to support the investigation and remediation activities. This may include:

- Audit logs of all software involved
- Witness statements
- Tapes/discs/drives containing audit logs and the data that was compromised
- Technical architecture in place at the time of the breach and other relevant software or system configuration documentation

2) Based on the findings of the investigation, the IT team will determine short term and long term remediation strategies which are documented in a Privacy and Security Breach Management Report. The report, including the recommendations emanating from the investigation, shall be approved by the Managing Director and implemented within the stated time frame.
3) Once a root cause, proposed resolution or workaround is identified, Zone1 IT team will test/validate and implement the appropriate resolution. The execution of the resolution must ensure that it considers existing change management processes.
4) If the plan also includes disciplinary actions for staff, Human Resources must be involved to take appropriate action.
5) If staff training is part of the remediation plan, training requirements should be defined and implemented.
6) Once the privacy breach is resolved, the CPSO will notify the affected client(s) and will provide a report of the incident.

Incident Response Procedure performed by the IT team

Step	Description
1.0	IT or DevOps typically become aware of a security incident first or it is reported to this group by others. In addition, security logs must be reviewed at least daily and that follow-up to exceptions is required. These logs must include the review of IDS, AntiVirus and all other security related devices.
2.0	Upon receiving the notification, IT team will validate the incident and rank it based on impact in terms of Confidentiality, Integrity and Availability to impact related systems.
3.0	Decision on course of action is based on the severity of the incident and whether any of our systems or data is actually compromised. Medium and High incidents require the assembly of the IT team, small and insignificant issues are resolved via regular clean up approach. To further assist in the categorization of the incident use the following factors. **Categorization of an Incident** – IT team will categorize the severity of an incident based on a series of factors including but not limited to the following: • Location and environment of systems impacted (e.g. production, staging, test, development, internal network, external network perimeter, etc.); • Number of systems impacted; • Type of system and /or information impacted; • Impact to revenue generation for the organization (e.g. incident causes revenue deferral or loss); • Impact to operational capabilities for the organization (e.g. incident prevents normal operations); • Relation to financial reporting capabilities for the organization (e.g. incident prevents timely reporting of financials to external auditors or regulatory bodies)
4.0	The IT team will bring all relevant team members together for the incident.
5.0	Clean, remove incident using in place tools and resources.

Step	Description
6.0	The IT team analyzes the impact of the incident and communicates any required outages to internal teams and external vendors. Evidence Preservation Activities: • Contain and Limit exposure and minimize data loss – The CSIRT should preserve evidence for investigative purposes by: • Not accessing or altering suspected/confirmed compromised systems – Do not logon, do not change passwords, and do not alter the systems in any deliberate way. • Isolate compromised systems from the network – Do not power off the machine or virtual machine (either by hard booting or graceful shutdown), instead disconnect the network cable or disconnect networking. • Immediately preserve all other evidence that may be of benefit to an investigation including upstream server logs, firewall/security logs and configurations, security events on other systems, etc. • Document in detail all actions taken above.
7.0	Update Customers and disable any related services as needed. Examples of External Vendors and clients etc.
8.0	Respond to outage requirements and disable any related services as needed.
9.0	The IT team contains repairs and protects the systems from recurrence. the IT team communicates the completion of these activities to internal teams and clients to bring systems and users back online.
10.0	Communicate to need to know team members within Zone1.
11.0	Restore services to affected systems .
12.0	A formal report outlining the incident, fix, and affected systems/data is provided to the Managing Director for review. Upon completion of this incident, there will be a post-mortem analysis to modify or evolve the incident response plan according to lessons learned and to incorporate industry developments.
13.0	Where it is suspected or confirmed that a data loss data has occurred, the organization is obligated to notify customers, clients, law enforcement and media (if greater than 500 records).
14.0	Review incident size and provide ruling on next steps.

[1] External malicious agents include hackers, identity thieves, hacktivists, foreign governments, and other potentially malicious agents that may attack Zone1 from the Internet.

Information Security Policy

1 Purpose

The purpose of this Information Security Policy is to provide guidance to the leadership, employees and contractors of Zone1 on matters concerning the management of information security. This includes:

a) Ensuring the protection of all Zone1 information system assets (including but not limited to all computers, mobile devices, networking equipment, software and data) and the mitigation of risks associated with the theft, loss, misuse, damage or abuse of these assets.

b) Making certain that users are aware of, and comply with, all current and relevant Canadian and US security and privacy regulations.

c) Providing a safe and secure working environment for staff, contractors and other authorized users.

d) Ensuring that all users understand their own responsibilities for protecting the privacy, confidentiality, availability and integrity of the data they handle.

e) Protecting Zone1 and its customers from liability or damage through the misuse of its IT cloud facilities, products and services.

f) Responding to feedback about this policy and updating as appropriate, initiating a cycle of continuous improvement.

2 Scope and Applicability

This Information Security Policy applies to:

1. All employees, contractors and agents of Zone1 who have access to or work in proximity to media or devices containing customer data.
2. All customer organizations and their respective agents who may have access to, and use, Zone1 information system assets.
3. All Zone1 information system assets including, system administration and security data, hardware, software, communications networks and facilities.
4. All activities associated with the operation of Zone1 information systems.

Please note that Zone1 does not collect or retain PHI data.

3 Principles

1. Zone1 shall comply with all applicable security, privacy or data protection laws and associated regulations or rules in all jurisdictions where Zone1 conducts business.
2. Zone1 adopts Security controls will be implemented as required based on an assessment of security risk. This may include controls in the areas of:
    a. Risk Assessment and Treatment.
    b. Security Policy.
    c. Organization of Information Security.
    d. Asset Management.
    e. Human Resources Security.
    f. Communications and Operations Management.
    g. Access Control.
    h. Information Systems Acquisition, Development and Maintenance.
    i. Information Security Incident Management.
    j. Business Continuity Management.
    k. Compliance with Laws, Policies and Standards.

4 Roles and Responsibilities

1. The Managing Director of Zone1 is responsible for ensuring that Zone1 is in compliance with applicable laws, regulations and rules, and with the security and privacy policies.
2. The Managing Director of Zone1 is responsible for the implementation of the Information Security Management Program (ISMP), including the review and approval of security policies.
3. The Managing Director will oversee the IT team in the following:
    a. Developing and maintaining information security policies and procedures.
    b. Ensuring that all employees and contractors are trained in security procedures and understand their responsibilities for the protection of data and critical information system assets.
    c. Detecting and investigating security and privacy incidents and taking appropriate corrective action.
    d. The application of reasonable security measures to protect data against unauthorized access, collection, use, disclosure, retention or disposal and to ensure the availability and integrity of data.
    e. Monitoring access to Data by authorized agents and users to detect unauthorized access, use and disclosure.
    f. Monitoring systems for attacks by malicious agents through the Zone1 monitoring and audit program.
    g. Developing, testing and maintaining a business continuity plan to ensure minimal disruption to health services in the event of a catastrophic system failure.
    h. Ensuring that necessary safeguards to protect the Zone1 Systems against threats identified in Threat and Risk Assessments (TRAs,) penetration tests and vulnerability assessments are implemented.
    i. Identifying, evaluating, and documenting all Zone1 information system assets, including, systems administration and security data, hardware, software and communications facilities and assign levels of sensitivity, criticality and ownership to them.
    j. Ensuring that Zone1 information systems are configured and maintained in accordance with security policies, standards and procedures.
    k. Ensuring that appropriate agreements are in place with suppliers, vendors or contractors, addressing roles and responsibilities for the protection of data and other sensitive information.

4. All employees, contractors and agents of Zone1 are responsible for:
    a. Understanding and following all security policies and procedures established by Zone1.
    b. Safeguarding the privacy and confidentiality of data collected, used, and disclosed in the course of their duties.
    c. Acting in a timely and co-operative manner to prevent, detect, and respond to security breaches or other incidents.
    d. Protecting their passwords and other devices (e.g. keys, access cards, access tokens) that enable access to Zone1 systems.

Password Policy, If not managed through the clients' authentication mechanism such as Active Directory.

1. Minimum password length is 8 characters.
2. Has at least one digit.
3. Has at least one alphabet character.
4. Has at least one upper case and lower-case alphabet character.
5. Has at least one symbol.
6. Does not repeat any of the previous 5 passwords.
7. Password expire every 90 days.
8. Inactive users account for 120 days is disabled. Password and UID reset are required to re-instate the account.

Tokens expiry

Tokens will expire based on the following timelines:

- In 2 hours in Dev Cluster
- In 2 hours in Production Cluster (not configurable by Partner)
- After browser tab is closed the token will be invalidated after at most 300 seconds

Brute force protection

User accounts will be locked after 5 unsuccessful login attempts after which the user must unlock by:

- Resetting their password through app/dashboard
- Waiting for 30mins (or whatever the configured time is)
- Admin user unlocking their account using the dashboard

5 Information Security Management Program

Management shall demonstrate leadership and commitment with respect to the information security management program by:

1. Ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization.
2. Ensuring the integration of the information security management system requirements into the organization's processes.
3. Ensuring that the resources needed for the information security management system are available.
4. Communicating the importance of effective information security management and of conforming to the information security management system requirements.
5. Ensuring that the information security management system achieves its intended outcome(s).
6. Directing and supporting IT team to contribute to the effectiveness of the information security management system.
7. Promoting continual improvement.
8. Supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

6 Policy Compliance

1. **Compliance Measures**

   The Zone1 IT team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits as needed.

2. **Exceptions**

   Any exception to this policy must be approved by the Managing Director in advance.

3. **Non-Compliance**

   - Any violation of this Information Security Policy by an employee of Zone1 is subject to disciplinary sanctions, as determined by Zone1 up to and including dismissal.
   - Any violation of this policy by an employee or agent of a customer organization will be reported to the customer organization and handled in accordance with the customer organization's sanctions policy. Where the violation poses a threat to Zone1 or other customers, Zone1 may take appropriate action to protect data and other sensitive assets. This could include suspension of access privileges for individuals who violate this policy.
   - Any violation of this Information Security Policy by a supplier, vendor or contractor or their respective employees and agents, is subject to remedies identified in the agreement or contract. Zone1 may request the removal of a supplier, vendor or contractor employee who has violated this Information Security Policy.

7 Contact

For more information about this Information Security Policy, please contact: **ZONE1 INTELLECT INC.**
1100 Burloak Drive, Suite 300, Burlington, Ontario L7L 6B2 | CANADA | info@zone1.ca | 888.886.0666

High-level Security Questionnaire

	Question	Answer	Notes
1	Will the system be hosted external to the Client's network, or will the system be hosted internal to the Client's network using vendor developed software?	External	
2	What is the location of the primary data center (if U.S., City, State - if outside the U.S., City, Country)?	Amazon Cloud (AWS)	Montreal, Canada
3	Will Client's be leasing a line and/or leasing and housing any communications routing equipment for the recovery center from the vendor?	No	
4	If using a 3rd party for production or alternate data, is the equipment part of a shared services agreement or if it is dedicated equipment.	Not applicable	
5	Do you allow client participation in your exercises?	Yes	
6	Will the pricing proposal include all items related to continuity and recovery as a separate line item?	Yes	
7	Is the vendor provides a service that will be or is accessible from potential client's website or that is ATM related?	No	
8	Are authentication controls applicable to high-risk online transactions involving access to customer information or the movement of funds to other parties?	Not applicable	
9	What access level tiers will be implemented? (user, view only, manager, administrator, etc.)	User and admin	
10	Will client's employees authenticate to the system?	No	
11	Is any sensitive corporate information stored in the system and if so, in what form?	No	
12	Who maintains ownership of the data?	Client	

	Question	Answer	Notes
13	Will the vendor require remote access to the Client's network for implementation and ongoing support?	No	
14	Will any known sub-vendors be used by the primary vendor to process or house customer data, and will the sub-vendors be held to the same contractual obligations as the primary vendor?	No	
15	Does the application require client software to be installed on the user workstations?	No	
16	What browsers are supported?	All	
17	For browsers supported, are you within 2 major releases?	Yes	
18	Does the vendor have a formal and documented security policy, standards, plans, and procedures? If so, are they available for review?	Yes	
19	Does the vendor conduct the following pre-employment screenings:		
A	Criminal Background checks (local, state, national, and international)?	Yes	
B	Credit backround checks?	No	
C	Drug screening?	Yes	
D	Biometric scans (e.g. fingerprint, retinal scans)?	No	
E	Do employees sign and abide by a non-disclosure agreement?	Yes	
20	Do you immediately remove, or modify access, when personnel terminate, transfer, or change job functions?	Yes	
21	Are employees have unique UID's on the Jump server in place to access the console?	Yes	
22	Do you authorize and establish employss's access based on user's job responsibilities and job functions?	Yes	

	Question	Answer	Notes
23	Do you periodically review employee access and ensure the access is appropriate?	Yes	
24	Do you terminate an electronic session after a predetermined time of inactivity?	Yes	ssh, Database, AWS, Client sessions time out is 15 minutes.
25	Do you implement system event logging on all servers and records at a minimum who, what, and when for all transactions?	Yes	Logging and monitoring tool is implemented and maintained through the separate monitoring server.
26	Do you retain an audit log for at least 90 days?	Yes	
27	Do you have a written Computer Security Incident Response Procedure?	Yes	
28	Do you have a written Information Security Policy?	Yes	
29	Do you have written backup procedures and processes?	Yes	AWS Snaphots, CPanel internal backup, CPanel external bckup on Acronis Cloud.
30	Do you store backup media in a secure manner and restrict access to the backup media to authorized individuals?	Yes	Acronis Cloud.
31	Do you prohibit the use of production data in the development or testing environment?	Yes	
32	Do you have encryption for confidential information being transmitted on external or Internet connections?	SSL encryption TLS 1.2 (Data transfer in transit)	No confidential data for encryption (Data at rest in database).
33	Do you Two Factor Authentication (2FA) to access the production server?	Yes	Via AWS and ssh key via shell.
34	Do you enforce a password policy that requires a password to have a minimum of 8 characters, expire every 90 days and have complexity requirements?	Yes	For server and AWS console access.

	Question	Answer	Notes
35	Do you prohibit passwords to be stored in clear text or easily decipherable?	Yes	
36	Do you have the account lockout feature enabled on your information systems?	Yes	
37	Do you shre or incinerate printed confidential information with a third party service provider?	No	
38	Do you remove all unnecessary services and default vendor accounts from computers?	Yes	
39	Do you change or disable all vendor-supplied default passwords on tools or systems used	Yes	
40	Do all servers have properly configured commercial anti-malware software installed and running at all times?	Yes	BitDefender endpoint security (Detecting trojans, viruses, malware & other malicious threats).
41	Are the system admins and privileged accounts activities logged?	Yes	
42	Do you sign a confidentiality agreement with your business associates before confidential information is disclosed?	Yes	
43	Do you have a business associate agreement signed by each of your business associates?	Yes	
44	Do you perform regular data and configuration backups on systems, to prevent customer information loss in the event that the original data becomes unavailable?	Yes	
45	Do you have security controls to detect or prevent phishing, spoofing or malware carrying email?	Yes	
46	Do you perform analytics on data or activities of the customer using the service?	Yes	For performance/ analytics reasons.
47	If analytics are being performed, are those analytics aggregated with the data of other customers of the vendor?	Yes	Only for Zone1 overall activities reports.
48	Are those analytics provided or sold to any other entities?	No	

Vulnerable Code Disclosure Statement

CVE-2021-44228 vulnerability

At Zone1, we do not use LDAP services or log4j-core.

Zone1 uses AWS cloud to host the platforms, Amazon SES for platform eCard sending, and google mail services for corporate communications, which are not impacted by CVE-2021-44228 vulnerability.

Security Awareness Training Statement

Since the rapid technology changes the world around us, Zone1 Intellect believes that the connection between the knowledge and the rapid technology is a must for the success of its business module.

Zone1 Intellect relies on full-time contractor developers to enhance and administer its services.

As part of the screening process, we ensure that developers are well trained and up to date with security and privacy practices related to SOC 2 and 27K and the privacy legislation.

On an annual basis, Zone1 Intellect verifies with the contractors that they have attended at least one security refreshing course, and they are aware of the latest security measures.

ZONE1 INTELLECT INC.
Corporate Executive Office
1100 Burloak Drive, Suite 300
Burlington, Ontario L7L 6B2 | CANADA
888.886.0666 | info@zone1.ca | zone1.ca