ADDENDUM
CYBERSECURITY AND INFORMATION SECURITY POLICIES AND OPERATIONS OF IRONYUN

1. IronYun VP of Operations & IT is responsible for the cybersecurity & information security of IronYun operations. His/her duties include but are not limited to:
    - Facilitate the confidentiality, integrity, and availability of data
    - Reduce the risk of security incidents, including cyberattacks and phishing attempts
    - Execute security programs across the organization

2. Device policy:
    2.1. BYOD policy is allowed, where the employees are held responsible for protecting the security of all data and communications as subjected to NDAs between the employees and IronYun, and between IronYun and partners/customers.
    2.2. Google Mobile & endpoints management and Google Security Checkup are used to manage company-issued devices.
    2.3. Each IronYun employee with remote access to the local environment and application is provided with a secured account, and the system logs the login of the accounts.
    2.4. Software installation for Vaidio design, production, training and testing is only allowed on company servers in the local environment.
    2.5. Only the teams responsible for a certain set of tasks have user access to the servers/software for that set of tasks.
    2.6. Bitlocker/Innodisk Hardware-based AES Encrypted Storage is used for device encryption.
    2.7. HiNet enterprise information security service is used for malware protection. The activities performed include, but are not limited to:
        - DDoS Protection
        - Virus Blocking
        - Intrusion Detection & Prevention
        - Malicious website blocking
    2.8. Lockout policy:
        - Server hardware logon will lock out for 30 seconds after three failed attempts with a wrong IPMI password.
        - The VPN account will be locked out after five failed attempts of Array VPN login.
        - Vaidio login will be locked out for at least 1-3 minutes if a wrong-password DDoS attack is detected.
    2.9. All mobile and computing devices that connect to the internal network must comply with the Minimum Access Policy (page 20)

    2.10. IronYun employees shall avoid downloading any data and information of and/or about IronYun and IronYun's customers from IronYun's secured data-sharing platform to personal devices unless absolutely necessary (such as presentation materials for offline events)

Digitally signed by Bîrsan Vitalie
Date: 2025.07.10 09:30:55 EEST
Reason: MoldSign Signature
Location: Moldova
MOLDOVA EUROPEANĂ

2.11. IronYun employees shall remove all IronYun's and IronYun's customer's information and data from personal devices as soon as the activity that requires the download is completed, so that such information cannot be recovered

3. The following devices & measures are used for the External Devices or Remote Access security:
    - FW - Palo alto PA-3020 / FortiGate 100D
    - VPN - Server Array Networks / MotionPro Clients
    - AWS VPN : AWS Virtual Private Network
        - AWS Client VPN
        - AWS Site-to-Site VPN
    - MFA:
        - Google 2-Step Verification / Authenticator / SMS
        - Vasco IDENTIKEY
        - Hubspot 2-Step Authentication

4. Information Security Awareness, Education and Training:

    4.1. IronYun provides regular information security training to all employees

    4.2. All IronYun employees are aware of and use security measures to avoid phishing campaigns

    4.3. IronYun provides regular information security training to the individuals responsible for management

    4.4. IronYun periodically checks the actual status of compliance with information security rules, by requesting all employees to perform self-inspection checks. The designated management personnel oversees the improvement of any nonconformities

    4.5. IronYun has a confidentiality section in the work rules or other regulations and obtains a commitment to confidentiality from employees

5. Asset management policy:

    5.1. Asset Management Policy is to establish the rules for the control of hardware, software, applications, and information used by IronYun.

    5.2. All hardware, software, and applications must be approved, inventoried, and purchased by IronYun OPIT.

    5.3. Software used by IronYun employees, contractors, and/or other approved third parties working on behalf of IronYun must be properly licensed.

    5.4. Only authorized cloud computing applications may be used for sharing, storing, and transferring confidential or internal information.

5.5. The use of cloud computing applications must be done in compliance with all laws and regulations concerning the information involved, e.g., personally identifiable information, protected health information, corporate financial data, etc.

5.6. Two-factor authentication is required for external cloud computing applications with access to any confidential information for which IronYun has a custodial responsibility unless a waiver/exception form is formally approved.

5.7. Contracts with cloud computing application providers must address data retention, destruction, data ownership, and data custodian rights regarding stored IronYun data.

5.8. Hardware, software, and application inventories must be maintained continually.

5.9. A general inventory of information (data) must be mapped and maintained on an ongoing basis.

5.10. All IronYun assets must be formally classified with ownership assigned.

5.11. IronYun assets exceeding a set value, as determined by company or IT management, are not permitted to be removed from IronYun's physical premises without management approval.

5.12. All IronYun physical assets exceeding a set value, as determined by management, must contain asset tags or a similar means of identifying the equipment as being owned by IronYun.

5.13. Confidential information must be transported either by a designated IronYun employee or a courier approved by IT management.

5.14. Upon termination of employment, contract, or agreement, all IronYun assets must be returned to IronYun management or leadership and documented accordingly.

6. Data classification policy - IronYun establishes a framework to classify data based on its sensitivity, value and criticality to the organization, so sensitive corporate and customer data can be appropriately secured .

Classes of data, determined by sensitivity	**Data types**	**Security Level**
Confidential	Product development data: IronYun's intellectual property, including all source codes and default models for all customers' use	Critical

Internal	IronYun organization data: including employee information, inventory information, accounting data, etc. Customer data: for model training and model/engine testing	
Public	Publicly available data used and processed by Vaidio to display in demos, such as data from Earthcam streams	High

7. Confidential management of information assets:
    - IronYun regularly identifies and inventories sensitive information
    - When reproducing or duplicating any confidential information in compliance with the relevant agreement, IronYun maintains the reproduced or duplicated confidential information in the same manner as the original
    - IronYun manages confidential information separately from other information

7.2. Disposing of confidential information:
- In the case of electronic information, IronYun employees completely erase all confidential information stored on servers, personal computers, portable devices, and recording media
- In the case of information on paper (documents, drawings, etc.), IronYun employees properly shred, dissolve, or incinerate it
- In the case of embodiments (molds, prototypes, etc.), ironYun employees destroy it so that no confidential information can be discerned

7.3. Physical Management:
- IronYun has physical measures in place to restrict entry of unauthorized individuals to locations (premises, buildings, rooms) where confidential information is handled, such as access cards, badge locks, face recognition system
- Person responsible for management within their department allows only those who need to know confidential information in the course of their work to enter the area where such information is handled
- IronYun strategically locates and installs critical systems, equipment, and wiring related to confidential information to avoid damage from natural disasters such as earthquakes and man-made accidents such as tripping over cables
- IronYun ensures that paper information (documents, drawings, etc.) and embodiments (molds, prototypes, etc.) can only be accessed by those who need to know the information for business purposes and takes measures to prevent theft

7.4. Management of Information System User IDs:
- IronYun has established the following rules for managing user IDs for information systems:

- Prohibit information system users to share IDs with other users
- Establish procedures for issuing and approving user IDs for information systems
- Immediately delete IDs of retirees, transferees, and others who are no longer involved in related work, as well as temporary user IDs and other IDs that are no longer needed
- Periodically check that there are no unmanaged IDs

7.5. IronYun prohibits the installation and use of file exchange software (software with a high risk of information leakage) and regularly checks for the installation and use of such software

7.6. IronYun prohibits the transmission or sharing of confidential information via free email services (Yahoo! Mail, etc.) or data sharing services (Google docs, etc.)

8. Data destruction policy: On termination of the provision of Personal Data processing services, IronYun shall be under obligation to delete all Personal Data processed on behalf of Partner and certify to Partner that it has done so unless Union or Member State law or other law to which IronYun is subject requires further storage of the Personal Data by IronYun.

9. Access Management Policy:
   - Minimum Access Policy (page 20)
   - Password policy (page 22)

10. Cryptographic management policy: a) user passwords are encrypted (PBKDF2); b) SSL/TLS (AES 256) is used to protect the data transmission; c) user data and system data encryption rely on SSD encryption as described in Section 2.6.

11. Physical and environmental security policy: IronYun's VP of Operations (or designee) monitors a wide variety of possible risks that may affect IronYun. These risks include utility outages, building safety systems, security issues, weather, seismic activity, and market and finance volatilities. IronYun also has a proactive building maintenance program that is intended to prevent utility and equipment failures and malfunctions that could lead to a crisis. In addition, IronYun's staff conducts a wide variety of routine inspections of work areas and conditions to ensure that safety hazards are identified and corrected in a timely manner.

12. Endpoint security policy:

    11.1 Measures taken to maintain and update endpoint security solutions:

    - Regularly checking to see whether the endpoint security solution is up to date by routinely updating the program with the newest security patches and bug fixes
    - Looking for any shady activity on endpoints involving atypical account logins or sudden updates or downloads
    - Conducting routine malware and other malicious software checks on endpoints
    - Informing IronYun staff about the best internet security and safety practices, including employing solid passwords and eliminating phishing emails

- Using a solid firewall to stop malicious connections from getting to the endpoints
- Setting up automatic security updates
- Using two-factor authentication

11.2 Measures taken to handle endpoint security incidents and breaches:

- Identify and isolate the affected endpoint
- Assess the damage
- Contain the incident or breach
- Investigate the incident or breach
- Remediate the issue
- Communicate with stakeholders
- Learn from the incident or breach

11.3 Measures taken to handle endpoint security compliance requirements:

- Implement access control measures
- Monitor and audit endpoints
- Encrypt data
- Patch management
- Use application whitelisting
- Backup data

11.4 Measures taken to handle endpoint security in a remote work environment:

- Establish Security Protocols
- Monitor and Control Access
- Use a Virtual Private Network (VPN)
- Implement Firewall and Antivirus Software
- Educate Employees
- Restrict Unauthorized Access
- Monitor Network Activity

11.5 Measures taken to handle endpoint security for mobile devices:

- Verifying that all mobile devices' operating systems and security updates are current to reduce the possibility of security vulnerabilities.
- Using a mobile device management (MDM) service to manage a mobile device, which enables one to remotely modify device settings and impose security regulations such as encryption and password restrictions.
- Requiring IronYun employees to turn on two-factor authentication on their gadgets to prevent illegal access to gadgets.
- Ensuring that any private information saved to the gadget is encrypted.
- Establishing a security policy for mobile applications to ensure that any programs downloaded and installed on the device are safe and current.

13. Backup policy:

13.1. Full and incremental backups protect and preserve corporate network information and should be performed on a regular basis for system logs and technical documents that are not easily replaced, have a high replacement cost, or are considered critical.

13.2. Backup media should be stored in a secure, geographically separate location from the original and isolated from environmental hazards.

13.3. Backup network components, cabling and connectors, power supplies, spare parts and relevant documentation should be stored in a secure area on-site as well as at other corporate locations.

13.4. Data and document retention policies are established to specify what records must be retained and for how long.

13.5. All departments are responsible for specifying their data management, data retention, data destruction and overall records management requirements.

13.6. See the below sample for backup policies and backup plan

Service	Service Owner	Priority	Description	Service Location	OS or App	Data Size	Backup Frequency	Repository	Responsible for backup	Status
BITBUCKET	Ying-Chu	High	Source Code	bitbucket.org/Ironyun	SaaS	<200GB	Every Release Manually	Download and store in NAS://RD	Ying-Chu	
JIRA	Same	Medium	Development	Ironyun.atlass.net	SaaS	<200GB	Bi-Monthly Manually	Download and store in NAS://RD	Ying-Chu	
AI Training	Patrick	High	Training data set	Patrick's PC	MAC OS	1TB	Weekly Manually	Backup to AI-4 training machine	Patrick	
Jenkins	Same	Medium	Build/Rep server	172.16.15.10 172.16.15.109	Ubuntu	10TB	Daily-Auto	Download and store in NAS://RD	Same	
Figma	Karen	High	UIUE Specs.	www.figma.com	SaaS	<30GB	Every Release Manually	Download and store in NAS://RD	Karen	
Google drive Eng. folder	Karen	High	Eng. Data	Google Cloud	SaaS	<100GB	Daily- Auto	Download and store in NAS://RD	Karen	
ERP	Sonia	High	Sunlike ERP	172.16.15.55	WinSrv	1.26GB/ day	Auto-Daily/ Manual-Monthly	1. Sunlike general BF daily(Sonia) 2. RSync copy to BS via script daily	Leo	
							Daily			

14. Log management policy: IronYun's log management policy establishes processes to ensure that all relevant system logs are accessible and consistently monitored. All production systems within IronYun shall record and retain audit-logging information that includes the following information:

14.1. Vaidio logs:

- System log: analyze specific trends or record the data-based events/actions of the Vaidio system environment network. Three log types: INFO, WARN, ERROR
- Diagnostic log: encrypted log of hardware errors, processing consumption, analytic/alert/connection errors, failed login attempt from the IP address of the computer trying to access Vaidio
- Audit trail: successful user login/logout, time and user actions in the entire Vaidio system (such as camera activation/modification)

14.2. IronYun operations logs:

- Each team has a logging system to keep track of activities, inventory, tasks, etc.

14.3. IronYun support portal:

- Ticketing system for technical support and information; central log of support activities between customers and IronYun

15. Vulnerability and Patch Management process:

    Vaidio undergoes professional tests and vulnerability scans with each release to ensure software security and stability, while also ensuring customer satisfaction. For system security scans, tools like Trivy, Snyk, and Nessus are used. Please refer to the latest Vaidio Scan Report for more information.

16. Network security policy:

    16.1. Users are permitted to use only those network addresses assigned to them by Ironyun's IT Department OPIT.

    16.2. All remote access to IronYun will either be through a secure VPN connection on a IronYun owned device that has up-to-date anti-virus software, or on approved mobile devices

    16.3. Remote users may connect to IronYun Information Systems using only protocols approved by IT.

    16.4. Users inside the IronYun firewall may not be connected to the IronYun network at the same time a remote connection is used to an external network.

    16.5. Users must not extend or re-transmit network services in any way. A user must not install a router, switch, hub, or wireless access point to the IronYun network without IronYun IT approval.

    16.6. Users must not install network hardware or software that provides network services without IronYun IT approval. Non-IronYun computer systems that require network connectivity must be approved by IronYun IT.

    16.7. Users must not download, install, or run security programs or utilities that reveal weaknesses in the security of a system. For example, IronYun users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the IronYun network infrastructure. Only the IT Department is permitted to perform these actions.

17. Secure Software Development Lifecycle (SSDLC) policy: IronYun's Software Development Life Cycle (SDLC) includes the following phases:
    - Requirements Analysis
    - Architecture and Design
    - Testing
    - Deployment/Implementation
    - Operations/Maintenance

    During all phases, a secure SDLC involves integrating security testing and risk assessment into an existing development process. The following are the vulnerability management tests performed:

- Trivy (detects vulnerabilities of OS packages and application dependencies)
- Snyk (dependency scanner that improves developer security)
- Nessus (scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer connected to a network)
- Please refer to the latest Vaidio Scan Report for more information.

18. Secure coding training to developers: IronYun developers follow the most up-to-date best practices in coding to maximize code security. All codes are tested for vulnerabilities during and after development using the software tools mentioned in section 16. All security holes and potential bugs that may impact the security of the software codes are reviewed for every release, and critical/major risks will be addressed as soon as possible (including IronYun's product lines and third-party products that IronYun uses for development).

19. The last penetration testing performed by an external third-party company was completed on August 2023 by an end-user customer (a large multinational enterprise, whose name IronYun does not have permission to reveal due to the mutual NDA in effect).

20. Third-party/subcontractor management policy that includes third-party security checks deployed:
    20.1. IronYun Third-Party Management Policy:
        - IronYun makes every effort to assure all 3rd-party organizations are compliant and do not compromise the integrity, security, and privacy of IronYun or IronYun Customer data.
        - 3rd Parties include Customers, Partners, Subcontractors, and Contracted Developers.
    20.2. Policies to Assure 3rd Parties Support Organizational Compliance
        - The following are required before 3rd parties are granted access to any IronYun systems:
            - Due diligence with the 3rd party;
            - Controls implemented to maintain compliance;
            - Written agreements, with appropriate security requirements, are executed.
        - All connections and data in transit between the IronYun Platform and 3rd parties are encrypted end to end.
        - Access granted to external parties is limited to the minimum necessary and granted only for the duration required.
        - A standard business associate agreement with Customers and Partners is defined and includes the required security controls in accordance with the organization's security policies. Additionally, responsibility is assigned in these agreements.
        - IronYun has Service Level Agreements (SLAs) with Subcontractors with an agreed service arrangement addressing liability, service definitions, security controls, and aspects of service management.

- IronYun utilizes monitoring tools to regularly evaluate Subcontractors against relevant SLAs.
- Third parties are unable to make changes to any IronYun infrastructure without explicit permission from IronYun. Additionally, no IronYun Customers or Partners have access outside of their own environment, meaning they cannot access, modify, or delete anything related to other 3rd parties.
- Whenever outsourced development is utilized by IronYun, all changes to production systems will be approved and implemented by IronYun workforce members only. All outsourced development requires a formal contract with IronYun.
- IronYun maintains and annually reviews a list of all current Partners and subcontractors.
- IronYun assesses the security requirements and compliance considerations with all Partners and Subcontracts.
- Regular review is conducted as required by SLAs to assure security and compliance. These reviews include reports, audit trails, security events, operational issues, failures and disruptions, and identified issues are investigated and resolved in a reasonable and timely manner.
- Any changes to Partner and Subcontractor services and systems are reviewed before implementation.
- For all partners, IronYun reviews activity annually to assure that partners are in line with SLAs in contracts with IronYun.

20.3. Inventory and classification of outsourced products & services:

- If a product or service will be outsourced, both the due diligence during the selection process and the ongoing oversight of the selected vendor will be based on IronYun's assessment of the importance or criticality of the outsourced product or service, but all vendors will have some level of ongoing oversight.
- An inventory of third-party service providers shall be maintained, the inventory shall include:
  - Vendor risk level;
  - Types of data shared with the third party, including data classification;
  - Brief description of services; and
  - Significant controls in place.
- Vendor risk level assessment will be based on the following considerations:
  - A product/service will be designated "critical" if:
    - The vendor will be performing processing required for daily activities;
    - The vendor has access to Restricted/Sensitive information;
    - The service is significant to IronYun's strategic plans; and
    - executive management designates it as such.
  - A product/service will be designated "major'' if:
    - The vendor will perform any processing for IronYun;
    - The product is important to IronYun's competitive posture; and

        - Executive management designates it as such.
    - A product/service will be designated "low" if:
        - • The service is minimal to IronYun's strategic plans;
        - • The vendor's own reputation does not harm IronYun's reputation; and
        - • Executive management designates it as such.

20.4. Third Party Contracts. Formal contracts that address the relevant security and privacy requirements must be in place for all third parties that process, store, or transmit confidential data or provide critical services. The following must be included in all such contracts:

- Contracts will acknowledge that the third party is responsible for the security of the institution’s confidential data that it possesses, stores, processes, or transmits;
- Contracts stipulate that the third-party security controls are regularly reviewed and validated by an independent party;
- Contracts identify the recourse available to IronYun should the third party fail to meet defined security requirements;
- Contracts establish responsibilities for responding to direct and indirect security incidents including timing as defined by service-level agreements (SLAs);
- Contracts specify the security requirements for the return or destruction of data upon contract termination;
- Responsibilities for managing devices (e.g., firewalls, routers) that secure connections with third parties are formally documented in the contract: and
- Contracts stipulate geographic limits on where data can be stored or transmitted.

20.5. Third-Party Review. In all cases where IronYun’s sensitive, critical services or data are provided to a third-party service provider, IronYun must review the service provider's internal control structure to ensure compatibility with IronYun Information Security requirements. The request and the results of the review should be provided to the Management Team. Once the relationship is established, an ongoing review of the service provider's internal controls structure is required on at least an annual basis. The evaluation of a third party may include the following items (if applicable):

- Audited financial statements, annual reports, SEC filings, and other available financial information;
- Significance of the proposed contract on the third-party’s financial condition;
- Experience and ability in implementing and monitoring the proposed activity;
- Cost analysis comparing the Vendor’s offering to other methods of performing the service, including the use of the other potential vendors and performing the service in-house.
- Business reputation of the Vendor (including reference checks with current customers);
- Qualifications and experience of Vendor’s principals;

- Strategies and goals, including service philosophies, quality initiatives, efficiency improvements; and employment policies;
- Existence of any significant complaints or litigation, or regulatory actions against the Vendor;
- Ability to perform the proposed functions using current systems or the need to make additional investment;
- Use of other parties or subcontractors by the Vendor;
- Scope of internal controls, systems and data security, privacy protections and audit coverage;
- Business continuity and disaster recovery plans;
- Adequacy of management information systems;
- Insurance coverage.

21. Security Incident Management policy:

21.1. Security incident:

- Refers to an adverse event in an information system, and/or network, or the threat of the occurrence of such an event. Incidents can include, but are not limited to, unauthorized access, malicious code, network probes, and denial of service attacks.
- Security Incident Management at IronYun is necessary to detect security incidents, determine the magnitude of the threat presented by these incidents, respond to these incidents, and if required, notify IronYun members of the breach.

21.2. Program Organization:

- Computer Emergency Response Plans – IronYun management must prepare, periodically update, and regularly test emergency response plans that provide for the continued operation of critical computer and communication systems in the event of an interruption or degradation of service. For example, Charter connectivity is interrupted or an isolated malware discovery.
- Incident Response Plan Contents – The IronYun incident response plan must include roles, responsibilities, and communication strategies in the event of a compromise, including notification of relevant external partners. Specific areas covered in the plan include:
  - Specific incident response procedures
  - Business recovery and continuity procedures
  - Data backup processes
  - Analysis of legal requirements for reporting compromises
  - Identification and coverage for all critical system components
  - Reference or inclusion of incident response procedures from relevant external partners, e.g., payment card issuers, suppliers
- Incident Response Testing – at least once every year, the IT Department must utilize simulated incidents to mobilize and test the adequacy of response. Where appropriate, tests will be integrated with testing of

related plans (Business Continuity Plan, Disaster Recovery Plan, etc.) where such plans exist. The results of these tests will be documented and shared with key stakeholders.

- Incident Response and Recovery – A security incident response capability will be developed and implemented for all information systems that house or access IronYun controlled information. The incident response capability will include a defined plan and will address the seven stages of incident response:
    - Preparation
    - Detection
    - Analysis
    - Containment
    - Eradication
    - Recovery
    - Post-Incident Activity
- To facilitate incident response operations, responsibility for incident handling operations will be assigned to an incident response team. If an incident occurs, the members of this team will be charged with executing the incident response plan. To ensure that the team is fully prepared for its responsibilities, all team members will be trained in incident response operations on an annual basis.
- Incident response plans will be reviewed and, where applicable, revised on an annual basis. The reviews 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.
- Intrusion Response Procedures – The IT Department must document and periodically revise the Incident Response Plan with intrusion response procedures. These procedures must include the sequence of actions that staff must take in response to a suspected information system intrusion, who has the authority to perform what responses, and what resources are available to assist with responses. All staff expected to follow these procedures must be periodically trained in and otherwise acquainted with these procedures.
- Malicious Code Remediation – Steps followed will vary based on scope and severity of a malicious code incident as determined by Information Security Management. They may include but are not limited to: malware removal with one or more tools, data quarantine, permanent data deletion, hard drive wiping, or hard drive/media destruction.
- Data Breach Management – IronYun management should prepare, test, and annually update the Incident Response Plan that addresses policies and procedures for responding in the event of a breach of sensitive customer data.

- Incident Response Plan Evolution – The Incident Response Plan must be updated to reflect the lessons learned from actual incidents. The Incident Response Plan must be updated to reflect developments in the industry.

21.3. Program Communication:

- Reporting to Third Parties – Unless required by law or regulation to report information security violations to external authorities, senior management, in conjunction with legal representatives, the Security Officer, and the VP of IT must weigh the pros and cons of external disclosure before reporting these violations.
  - If a verifiable information systems security problem, or a suspected but likely information security problem, has caused third party private or confidential information to be exposed to unauthorized persons, these third parties must be immediately informed about the situation.
  - If sensitive information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, both its Owner and the Security Officer must be notified immediately.
- Display of Incident Reporting Contact Information – IronYun contact information and procedures for reporting information security incidents must be prominently displayed in public communication mediums such as bulletin boards, break rooms, newsletters, and the intranet.
- Member Notification – The notification will be conducted and overseen by IronYun's Director of Risk Management. The notification should contain, at a minimum, the following elements:
  - Recommendations for the member to protect him/herself
  - Contact information for the Federal Trade Commission
  - Contact information for the credit bureaus

22. IronYun conducts quarterly internal audits of information security prior to each product release and as needed in the event of security issues of related products by partner companies and vendors. The VP of Operations or his designee will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.