ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

Vendor Statement of Compliance
Data Privacy and Protection

This agreement is entered into between the Roseville City School District ("LEA" or "District") and Literacy Resources, LLC ("Service Provider") on 09/11/2023 ("Effective Date").

WHEREAS, the LEA and the Service Provider entered into an agreement for Educational Technology services;

WHEREAS, the LEA is a California public entity subject to all state and federal laws governing education, including but not limited to California Assembly Bill 1584 ("AB 1584"), the California Education Code, the Children's Online Privacy and Protection Act ("COPPA"), and the Family Educational Rights and Privacy Act ("FERPA");

WHEREAS, AB 1584 requires, in part, that any agreement entered into, renewed or amended after January 1, 2015, between a local education agency and a third-party service provider must include certain terms;

NOW, THEREFORE, the Parties agree as follows:

Section I: General - All Data

1. **PASSWORD SECURITY.** All passwords are considered secure. Vendors may not disseminate any passwords unless specifically directed by Educational or Technology Services management. Vendors will not provide information concerning Admin accounts (ROOT Admin, container Admin, local NT administrator or Domain administrator) or their equivalent to any persons. District personnel ONLY will disseminate this information. Vendors will never create "back door" or "generic" user accounts on any systems unless specifically directed to do so by LEA management.

   Agree: Yes ◉ No ○

2. **SYSTEM SECURITY.** Unauthorized access to or modification of District systems including file servers, routers, switches, NDS and Internet services is prohibited. Any attempt to bypass or subvert any District security system, both hardware, and software is prohibited.

   Agree: Yes ◉ No ○

3. **PRIVACY**. The vendor will adhere to all provisions of the Federal Family Educational Rights and Privacy Act (FERPA, 20 U.S.C. 123g), California Education Code and district policies regarding the protection and confidentiality of data. At all times, the vendor will consider all data collected in the course of their duties to be protected and confidential. Release of this data can only be authorized by Technology & Information Services management and state and federal law.

   Agree: Yes ◉ No ○

RCSD ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

Section I: General - All Data *(Continued)*

4. **REUSE**: Vendors shall not copy, duplicate, sell, repackage or use for demonstration purposes any Roseville City School District data without the prior, written consent of Educational or Technology Services management.

   Agree: Yes ◉ No ○

5. **TRANSPORT**: Vendor must provide a secure channel (S/FTP, HTTPS, SSH, VPN, etc) for the District to "push" data to the vendor and to extract data as required. Vendors will not have direct access to District systems and will not "pull" data at any time.

   Agree: Yes ◉ No ○

6. **EXTERNAL SECURITY:** Vendor must attach to this document reasonable evidence that their system is secure from external hacking and attacks. Devices such as firewalls and technologies such as NAT are the minimum requirements. Active IDS or similar technology is preferred.

   Agree: Yes ◉ No ○

7. **INTERNAL SECURITY:** Vendors must attach to this document reasonable evidence that their system is secure from internal hacking and attacks. Describe the interactions vendor personal (or their representatives) will have directly with District data. How is uploaded data from the District handled and processed? Who has access to this data? What happens to the data after the upload is complete? What security safeguards are in place to protected unauthorized access to District data? How are backup performed and who has access to and custody of the backup media? How long are backup maintained; what happens to the District data once the backup is "expired"? If any data is printed, what happens to these hard copy records?

   Agree: Yes ◉ No ○

8. **DISTRICT ACCESS:** Vendor must provide a secure means (see Item 5 above) for the District to extract ALL data from the vendor system. This can either be an online extraction tool or a vendor-provided extract as needed by the District (not to exceed quarterly). Describe the means and format of the data (delimited, Excel, MDB, SQL Dump).

   Agree: Yes ◉ No ○

9. **TERMINATION:** Upon termination of this agreement as provided herein, the vendor will permanently delete all customer data from their system as allowed by state and federal law. Vendor may be required to certify the destruction of LEA data within 90 days of contract termination.

   Agree: Yes ◉ No ○

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

Section II: AB1584 Compliance - Student Information Only

1. Vendor agrees that the Roseville City School District retains ownership and control of all student data.

   Agree: Yes ◉ No ○

2. Vendor must attach to this document a description of how student-created content can be exported and/or transferred to a personal account.

   Agree: Yes ◉ No ○

3. Vendor is prohibited from allowing third-parties access to student information beyond those purposes defined in the contract.

   Agree: Yes ◉ No ○

4. Vendor must attach to this document a description of how parents, legal guardians and students can review and correct their personally identifiable information.

   Agree: Yes ◉ No ○

5. Vendor will attach to this document evidence how student data is kept secure and confidential.

   Agree: Yes ◉ No ○

6. Vendor will attach to this document a description of procedures for notifying affected parents, legal guardians or eligible students when there is an unauthorized disclosure of student records.

   Agree: Yes ◉ No ○

7. Vendor certifies that student records will not be retained or available to a third party once the contract has expired or is canceled (See Page 2, Item 9).

   Agree: Yes ◉ No ○

8. Vendor will attach to this document a description of how they and any third party affiliates comply with FERPA.

   Agree: Yes ◉ No ○

9. Vendor and its agents or third parties are prohibited from using personally identifiable information from student records to target advertising to students

   Agree: Yes ◉ No ○

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

Section III: SB 1177 SOPIPA Compliance - Student Information Only

1. Vendors cannot target advertising on their website or any other website using information acquired from students.

   Agree: Yes (•) No ( )

2. Vendors cannot create a profile for a student except for school purposes as defined in the executed contract.

   Agree: Yes (•) No ( )

3. Vendors cannot sell student information.

   Agree: Yes (•) No ( )

4. Vendors cannot disclose student information unless for legal, regulatory, judicial, safety or operational improvement reasons.

   Agree: Yes (•) No ( )

5. Vendors must attach to this document evidence of how student information is protected through reasonable security procedures and practices.

   Agree: Yes (•) No ( )

6. Vendors must delete district-controlled student information when requested by the District.

   Agree: Yes (•) No ( )

7. Vendors must disclose student information when required by law, for legitimate research purposes and for school purposes to educational agencies.

   Agree: Yes (•) No ( )

As an authorized representative of my organization, I accept the conditions listed in this document.

Megan Rail 9-11-2023
Print Name

Megan Rail
Signature, Date

Laura Assem
Print Name (Roseville City School District)

9/11/23
Signature, Date (Roseville City School District)

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

EXHIBITS

Section 1.6: External Security

See attachment

Section 1.7: Internal Security

See attachment

Section II.2: Exporting of Student-Created Content

Not applicable. Students may not create content on the myHeggerty platform.

Section II.4: Review and Correcting Personally Identifiable Information (PII)

See attachment

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

EXHIBITS

Section II.5: Securing Student Data

See attachment

Section II.6: Disclosure Notification

See attachment

Section II.8: Family Educational Rights and Privacy Act (FERPA) Compliance

See attachment

Section III.5: How Student Data is Protected:

See attachment

Reset Form

Information Security Policy

Contents

1 Introduction

The Information Security Program (ISP) provides definitive information on the prescribed measures used to establish and enforce the information security and compliance program at Literacy Resources, LLC. ("Heggerty").

Heggerty is committed to protecting its employees, partners, clients from damaging acts that are intentional or unintentional. Effective security is a team effort involving the participation and support of every vendor that interacts with Heggerty data and/or systems. Therefore, it is everyone's responsibility, including employees, contractors, or vendors to be aware of and adhere to Heggerty's information security policy requirements.

Protecting Heggerty data and the systems that collect, process and maintain this data is of critical importance. Therefore, the security of systems must include controls and safeguards to offset possible threats, as well as controls to ensure the confidentiality, availability and integrity of the data:

Commensurate with risk, information security and privacy measures must be implemented to guard against unauthorized access to, alteration, disclosure or destruction of data and systems. This also includes protection against accidental loss or destruction. The security of systems must include controls and safeguards to offset possible threats, as well as controls to ensure confidentiality, integrity, and availability:

- **CONFIDENTIALITY** – Confidentiality addresses preserving restrictions on information access and disclosure so that access is limited to only authorized users and services.
- **INTEGRITY** – Integrity addresses the concern that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
- **AVAILABILITY** – Availability addresses ensuring timely and reliable access to and use of information.

Security measures must be taken to guard against unauthorized access to, alteration, disclosure or destruction of data and systems. This also includes against accidental loss or destruction.

2 Purpose

The purpose of the Information Security Program (ISP) is to prescribe a comprehensive framework for:

- Creating an information security and compliance program in accordance with Payment Card Industry Data Security Standards (PCI DSS).
- Comply with laws and regulations that apply to Heggerty.
- Protecting the confidentiality, integrity, and availability of Heggerty data and information systems.
- Protecting Heggerty, its employees, and its clients from illicit use of Heggerty information systems and data.
- Ensuring the effectiveness of security controls over data and information systems that support Heggerty's operations.

3 Scope & Applicability

These policies, standards, and procedures apply to all Heggerty data, information systems, activities, and assets owned, leased, controlled, or used by Heggerty, its agents, contractors, or other business partners on behalf of Heggerty. These policies, standards, and procedures apply to all Heggerty employees, contractors, sub-contractors, vendors, and their respective facilities supporting Heggerty business operations, wherever Heggerty data is stored or processed, including any third-party contracted by Heggerty to handle, process, transmit, store, or dispose of Heggerty data.

Some policies are explicitly stated for persons with a specific job function (e.g., an Information Security Officer); otherwise, all personnel supporting Heggerty business functions shall comply with the policies. Heggerty's IT Department has the authority to create exceptions to this policy. An Exceptions To Policy form is included in Appendix A

These policies do not supersede any other applicable law, higher-level company directive or existing labor management agreement in effect as of the effective date of this policy.

Heggerty reserves the right to revoke, change, or supplement these policies, procedures, standards, and guidelines at any time without prior notice. Such changes shall be effective immediately upon approval by management, unless otherwise stated.

4 Violations

Any Heggerty user found to have violated any policy, standard or procedure may be subject to disciplinary action, up to and including termination of employment. Violators of local, state, Federal, and/or international law may be reported to the appropriate law enforcement agency for civil and/or criminal prosecution.

5 Glossary – Key Terminology

The following terms are used in the policies and procedures:

Cardholder Data Environment (CDE): The people, processes and technology that directly store, process, or transmit cardholder data (CHD) or sensitive authentication data (SAD).

Heggerty Processing Environment (Processing Environment) : The people, processes and technology used to process the tokenized data in the Rackspace environment

Control: A term describing any management, operational, or technical standard, procedure or method that is used to manage risk. Controls are designed to monitor and measure specific aspects of standards and procedures to assist Heggerty in accomplishing stated goals or objectives.

Control Applicability: A term describing the scope in which a control or standard is relevant and applicable.

Control Objective: A term describing targets or desired conditions to be met that are designed to ensure that policy intent is met. Where applicable, Control Objectives are directly linked to an industry-recognized practice to align Heggerty with accepted standards or requirements.

Data: A term describing an information resource that is maintained in physical or digital format. Data may be accessed, searched, or retrieved via electronic networks or other electronic data processing technologies.

Data Owner: A term describing a person or entity that has been given formal responsibility for the security and privacy of a data asset, data asset category, or the data hosted on the asset. It does not mean that the asset belongs to the owner in a legal sense. Asset owners are responsible for making sure that data assets are secure and private while they are being developed, produced, maintained, and used.

Encryption: A term describing the conversion of data from its original form (clear text) to a form (cypher text) that can only be read by someone that can reverse the encryption process (decryption). The purpose of encryption is to prevent unauthorized disclosure of data.

Guidelines: A term describing recommended practices that are based on industry-recognized practices. Unlike Standards, Guidelines allow users to apply discretion or leeway in their interpretation, implementation, or use.

Information Security: A term that covers the protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. The focus is on the Confidentiality, Integrity, and Availability (CIA) of data.

Information System: A term describing an asset; a system, process, or network that can be defined, scoped, and managed. Includes, but is not limited to, computers, workstations, laptops, servers, routers, switches, firewalls, and mobile devices.

Least Privilege: A term describing the theory of restricting access by only allowing users or processes the least set of information access privileges necessary to accomplish a specific job or function.

Information Security Officer: A term used to describe a Heggerty member who is responsible for security and availability of information systems.

Periodic and Periodically: The PCI DSS uses the terms 'periodic' and 'periodically' in a number of places and it is up to Heggerty to define what those periods are for those requirements using those terms.

Policy: A term describing a formally established requirement to guide decisions and achieve rational outcomes. Essentially, a policy is a statement of expectation that is enforced by standards and further implemented by procedures.

Procedure: A term describing an established or official way of doing something, based on a series of actions conducted in a certain order or manner. Procedures are the responsibility of the asset custodian to build and maintain, in support of standards and policies.

Developer: A term used to describe a Heggerty member who is responsible for the secure development of commercial applications.

Sensitive Data: A term that covers categories of data that must be kept secure and private. Examples of sensitive data include Personally Identifiable Information (PII), Electronic Protected Health Information (ePHI), and all other forms of data classified as Restricted or Confidential in **Appendix A:** Data Classification & Handling Guidelines.

Sensitive Personally Identifiable Information (sPII): sPII is commonly defined as the first name or first initial and last name, in combination with any one or more of the following data elements: [1]

- Social Security Number (SSN) / Taxpayer Identification Number (TIN) / National Identification Number (NIN)

- Driver License (DL) or another government-issued identification number (e.g., passport, permanent resident card, etc.)
- Financial account number
- Payment card number (e.g., credit or debit card)

Significant Change: A change is considered 'significant' if it meets any one of the following criteria. When identified, this change will require the conduct of vulnerability scanning and penetration testing of the PCI in-scope environment.

- Changing devices such as firewalls, routers, switches and servers.
- Changes to payment applications.
- Upgrades or changes in operating systems. Upgrades and changes in operating systems should also be obvious as significant changes.
- Patching of operating systems or applications.
- Network changes.

Standard: This is the most technical and detailed of the document types, and lays out specific settings and parameters to use with specific technologies. For example the Build Standard for a Windows 2016 server would give values to be set for registry items, and specify that some system processes be disabled, and that certain features and components be uninstalled.

Target Audience: A term describing the intended group for which a control or standard is directed.

6 Information Security Program – Requirement 12

Heggerty shall protect the confidentiality, integrity, and availability of its data and information systems, regardless of how its data is created, distributed, or stored. Security controls will be tailored accordingly so that cost-effective controls can be applied commensurate with the risk and sensitivity of the data and information system, in accordance with all legal obligations.

Management Intent: The purpose of this policy is for Heggerty to specify the development, implementation, assessment, authorization, and monitoring of the information security program. The successful implementation of security controls depends on the successful implementation of Heggerty's program-level controls.

6.1 Publishing an Information Security Policy - Requirement 12.1

Control Objective: The organization establishes, publishes, maintains and disseminates a security policy.

Standard:

Heggerty's information security policies, procedures and standards are represented in a series of documents, the Information Security Program (ISP) has been:

- Endorsed by executive management; and
- Disseminated to the appropriate parties to ensure all Heggerty personnel understand their applicable requirements.

Heggerty's information security policies and standards shall be represented in a series of documents, the Information Security Program (ISP) that:

- Shall be reviewed and updated at least annually; and
- Disseminated to the appropriate parties to ensure all Heggerty personnel understand their applicable requirements.

6.2 Publishing an Acceptable Use Policy - Requirement 12.3

Control Objective: The organization establishes an acceptable use policy that communicates organization's standards for selection and usage of approved solutions

Standard: These Rules of Behavior apply to the use of Heggerty-provided IT resources, regardless of the geographic location:

- Data and information system use must comply with Heggerty policies and standards.
- Unauthorized access to data and/or information systems is prohibited.
- Users must prevent unauthorized disclosure or modification of sensitive information, including Personally Identifiable Information (PII).

6.2.1 Acceptable Use

Users shall:

- In accordance with Heggerty's procedures, immediately report all lost or stolen equipment, known or suspected security incidents, known or suspected security policy violations or compromises, or suspicious activity. Known or suspected security incidents are inclusive of an actual or potential loss of control or compromise, whether intentional or unintentional, of

authenticator, password, or sensitive information, including PII, maintained or in possession of the user.

- Ensure that software, including downloaded software, is properly licensed, free of malicious code, and authorized before installing and using it on Heggerty-owned information systems.
- Log off or lock systems when leaving them unattended.
- Complete security awareness training before accessing any information system and on an annual basis thereafter. Permit only authorized users to use Heggerty provided information systems.
- Secure sensitive information (on paper and in electronic formats) when left unattended.
- Keep sensitive information out of sight when visitors are present.
- Sanitize or destroy electronic media and papers that contain sensitive data when no longer needed, in accordance with Heggerty records management and sanitization policies, or as otherwise directed by management.
- Only access sensitive information necessary to perform job functions (e.g., need to know).
- Use PII only for the purposes for which it was collected, to include conditions set forth by stated privacy notices and published notices.
- Ensure the accuracy, relevance, timeliness, and completeness of PII, as is reasonably necessary.
- Wear Heggerty-issued identification badges at all times in Heggerty-operated facilities.

6.2.2 Prohibited Use

Users shall not:

- Direct or encourage others to violate Heggerty's policies, procedures, standards or guidelines.
- Circumvent security safeguards or reconfigure systems except as authorized (e.g., violation of least privilege).
- Use another user's account, identity, or password.
- Exceed authorized access to sensitive information.
- Cause congestion, delay, or disruption of service to any Heggerty-owned IT resource. For example, greeting cards, video, sound or other large file attachments can degrade the performance of the entire network, as can some uses of "push" technology, such as audio and video streaming from the Internet.
- Create, download, view, store, copy or transmit materials related to sexually explicit or sexually oriented materials.
- Create, download, view, store, copy or transmit materials related to gambling, illegal weapons, terrorist activities, illegal activities or activities otherwise prohibited.
- Store sensitive information in public folders or other insecure physical or electronic storage locations.
- Share sensitive information, except as authorized and with formal agreements that ensure third parties will adequately protect it.
- Transport, transfer, email, remotely access, or download sensitive information, inclusive of PII, unless such action is explicitly permitted by the manager or owner of such information.
- Store sensitive information on mobile devices such as laptops, smartphones, USB flash drives, or on remote systems without authorization or appropriate safeguards, as stipulated by organization policies.
- Knowingly or willingly conceal, remove, mutilate, obliterate, falsify, or destroy information for personal use for self or others.

- Use Heggerty-provided IT resources for commercial purposes or in support of “for-profit” activities or in support of other outside employment or business activity (e.g., such as consulting for pay, administration of business transactions, the sale of goods or services, etc.).
- Engage in any outside fund-raising activity, including non-profit activities, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity;
- Establish unauthorized personal, commercial or non-profit organizational web pages on Heggerty provided information systems.
- Use Heggerty-owned IT resources as a staging ground or platform to gain unauthorized access to other systems.
- Create, copy, transmit, or retransmit chain letters or other unauthorized mass mailings regardless of the subject matter.
- Use Heggerty-owned IT resources for activities that are inappropriate or offensive to fellow employees or the public. Such activities include, but are not limited to hate speech, harassment, bullying, intimidation or other abusive conduct that ridicules others on the basis of race, creed, religion, color, age, sex, disability, national origin, or sexual orientation.
- Add personal IT resources to existing Heggerty-owned information systems without the appropriate management authorization, including the installation of modems on data lines and reconfiguration of systems.
- Intentionally acquire, use, reproduce, transmit, or distribute any controlled information including computer software and data that includes information subject to the Privacy Act, copyrighted, trademarked or material with other intellectual property rights (beyond fair use), proprietary data, or export controlled software or data.
- Send anonymous messages.
- Remove Heggerty-proved IT resources from organization property without prior management authorization.
- Modify software without management approval.
- Post information on external blogs, social networking sites, newsgroups, bulletin boards or other public forums which:
    - Derogatory to Heggerty or its management;
    - Contrary to Heggerty’s mission or stated positions; or

6.2.3 Additional Security Rules For Privileged Users

Security and system administration personnel with elevated privileges have significant access to processes and data in information systems. As such, Security, Network, Systems, and Database Administrators have added responsibilities to ensure the secure operation of any Heggerty system.

Personnel with elevated privileges are to:

- Privileged accounts should only be used when elevated permissions are needed for a specific task. Instead of logging in as a super-user, or placing a user account in a group that provides privileged access, utilize operating system features such as “sudo” (Unix/OSX) or “Run As…” (Windows) which allow for temporary elevation of privileges.
- Heggerty will maintain an inventory of privileged accounts for critical Active Directory groups (such as Domain Admins), admin and root accounts for Unix servers, databases, and business applications. The inventory will identify the owner of each privileged account, the access

privileges granted, the system component it is associated with, the location of the device, and the contact info for the account owner.

- For privileged access, administrators will each use a unique account that is tied to their personal identity and is separate from their day-to-day user account. The default administrator, root or similar accounts will only be used when absolutely necessary;
- To minimize risk, Heggerty will enforce the principle of least privilege by granting employees the minimum privileges needed to perform their jobs (e.g., "full admin" vs. "Power user" vs. "regular user").
- Privileged account activity will be logged. Examples of events to log include:
    - The use of admin privileges (e.g. sudo logs)
    - Successful and failed admin login attempts or privilege escalation attempts
    - Account lockout events
    - Changes to privileged groups (e.g. addition of a user account to a privileged group)
    - Actions of privileged account usage

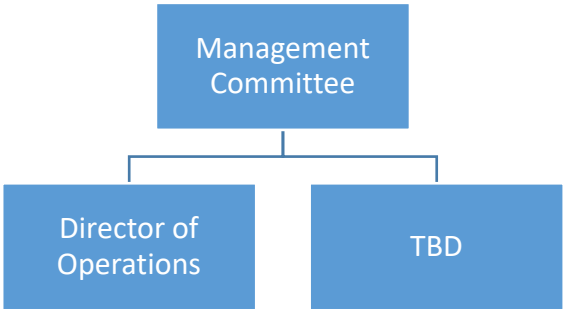
6.3 Assigned Information Security Responsibilities – Requirement 12.5

Control Objective: The organization appoints an individual assigned with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

Standard: Every user at Heggerty, regardless of position or job classification, has an important role, when it comes to safeguarding the Confidentiality, Integrity, and Availability (CIA) of the information systems and data maintained by Heggerty. It is important that every individual fully understands their role, their associated responsibilities, and abide by the security standards, policies, and procedures set forth by the Written Information Security Program (WISP).

Responsibilities shall be assigned based on "ownership" or stake-holding by the Information Security Officer (ISO).

Role and Description of Security Role with Description of Security Responsibilities:



6.3.1 Management Committee

The IT Governance Committee is a standing committee that is composed of Heggerty leadership to ensure strong executive-level buy-in to our philosophy of privacy and security first, and will be supported by the executive leadership, and the subject-specific valuestreams teams to action the numerous areas of compliance.

The IT Governance Team will jointly create an enterprise-wide approach to proactively identify, manage and monitor key risks to information and supporting IT infrastructure, and develop mitigation strategies that will be used to achieve business objectives.

6.3.1.1 GOALS AND OBJECTIVES

The IT Governance Committee's responsibilities include the following:

- Developing the IT strategy and roadmap for Heggerty
- Creation, approval and management of IT policies
- Incorporating privacy-by-design and security-as-default initiatives into Heggerty's infrastructure and applications
- Maintaining an effective IT governance program including:
    - Development and implementation of Heggerty IT governance policies, processes and procedures.
    - Development and implementation of relevant employee and contractor training on Heggerty IT policies and procedures.
    - Development and implementation of a breach notification incident response process including a triage process for breach determination and application of a harm threshold framework.
    - Establishing internal procedures and benchmarks to enhance the accuracy, security, and confidentiality of personal data which includes any information relating to an identified or identifiable person; and
    - Establishing mechanisms, such as procedures for access and redress, to protect the personal privacy rights of any individuals who are subject to the collection of personal data by Heggerty.
- Interpretation and application of Heggerty policy
- Escalating and/or approving of any IT governance issues.
- Notifying the senior management of :
    - Exceptions to policy implementation.
    - Any material risks to personal data held by Heggerty.
    - The likelihood of a breach occurring and any potential damage; and
    - Mitigating controls or safeguards to prevent risks or breach to Personal Data.
- Make recommendations to the senior management for investments to reduce or eliminate risks
- Provide frequent and effective updates to the senior management regarding:
    - Incidents/breaches including investigations and mitigating activities
    - Training updates
    - Non-compliance issues and sanctions

6.3.1.2 MEETINGS AND PROCEDURES

The IT Governance Committee shall meet at least monthly until the end of the 2022 calendar year and quarterly thereafter, with ad hoc meetings being called as necessary upon request by the Chair to the Committee.

6.3.2 Company Management (as of latest revision, CEO)

Responsibilities:

- Promote a security-first culture
- Ensure the company complies with its legal and regulatory obligations
- Approve the company's information security program policies and budget.;

- Ensure that the security program is properly observed by all personnel and that action is taken when personnel do not follow the program;
- Review results of risk assessment and take decisions related to risk treatment
- Appoint, in writing, an Information Security Officer (ISO) to implement the cybersecurity program;

6.3.3 Information Security Officer (as of latest revision, Director of Operations)

The ISO is accountable to the Heggerty's Management for the development and implementation of the information security and compliance program. The ISO will be the central point of contact for setting the day-to-day direction of the cybersecurity program and its overall goals, objectives, responsibilities, and priorities.

Responsibilities:

- Oversee, develop and maintain the company's information security program policies, standards and procedures including their dissemination to employees, contractors, and vendors who safeguard the company's information systems and data, as well as the physical security precautions for employees and visitors;
- Ensure an appropriate level of protection for all company owned or maintained information resources; whether retained in-house or under the control of contractors;
- Ensure that funding and resources are programmed for staffing, training, and support of the information security program and for implementation of system safeguards, as required;
- Ensure that persons working in a information security role are properly trained, and supported with the appropriate resources; and
- Provide a secure processing environment including redundancy, backup, and fault-tolerance services.
- Ensure an appropriate level of protection for the company's information resources; whether retained in-house or under the control of outsourced contractors;
- Issue the Heggerty Information Security Program policies and guidance that establish a framework for its information security program
- Ensure appropriate procedures are in place for security testing and evaluation for all information systems; and monitor, evaluate, and report to company management on the status of cybersecurity within the company;
- Ensure that persons working in a information security role are properly trained, and supported with the appropriate resources;
- Assist in compliance reviews and other reporting requirements;
- Promote best practices in cybersecurity management;
- Monitor and evaluate the status of the company's information security posture by performing periodic compliance reviews of the Heggerty Information Security Program and system controls (including reviews of security plans, risk assessments, and security testing processes);
- Assign ownership of resources.

6.3.4 Software Engineers

Under the direction of the ISO, Software Engineers are responsible for the implementation and management of the security of Heggerty's products and services.

Responsibilities:

- Include security considerations in applications systems procurement or development, implementation, operation and maintenance, and disposal activities (e.g., life cycle management);
- Plan and execute security assessments (dynamic testing, static testing, code review, etc) and threat modeling of Heggerty's products, services, and associated cloud infrastructure.
- Build and implement security solutions across the product life-cycle, such as standalone security tools, CI/CD pipeline integrations, and product security features.
- Contribute unified security requirements to product specifications.
- Work across various products to prioritize security features and bugs, and ensure implementation and mitigations.
- Act as SME on multiple information security areas (e.g. security architecture, application security, threat modeling etc.)
- Monitor threats and vulnerabilities impacting Heggerty's products and services, develop proof-of-concepts as appropriate, identify mitigations and assess/communicate associated risk.
- Assist in execution of 3rd-party audits, penetration tests, and bug bounty programs.
- Contribute to the creation and delivery of security training.
- Research emerging attack vectors and techniques.
- Handle and investigate incidents in cooperation with, and under direction of, the Information Security Officer (ISO)

6.3.5 Network Engineers

Under the direction of the ISO, Network Security Engineers are responsible for the technical implementation and management of network and infrastructure security controls, and for daily security operations.

Responsibilities:

- Develop and implement information security plans and policies
- Develop strategies to respond to and recover from a security breach
- Develop or implement open-source/ third-party tools to assist in detection, prevention and analysis of security threats
- Awareness training of the workforce on information security standards, policies and best practices
- Implement protections
- Installation and use of firewalls, data encryption and other security products and procedures
- Conduct periodic network scans to find vulnerabilities
- Conduct penetration testing, simulating an attack on the system to find exploitable weaknesses
- Monitor networks and systems for security breaches, through the use of software that detects intrusions and anomalous system behavior
- Investigate security breaches, and lead incident response, including steps to minimize the impact and then conducting a technical and forensic investigation into how the breach happened and the extent of the damage

6.3.6 End Users

All employees (and contractors) are considered both custodians and users of the information systems and data on their issued information systems and are required to uphold all applicable Heggerty Information Security Program (BL-ISP) policies, procedures, standards, and guidelines.

Responsibilities:

NOTE: end user's responsibilities center upon being aware of the sensitivity and proper handling method of sensitive information.

- Know and abide by all applicable policies and procedures;
- Complete all required user training and awareness programs;
- Understand and abide by the Rules of Behavior
- Know which systems or parts of systems for which they are directly responsible (desktop, browser, etc.);
- Know the sensitivity of the data handled by systems under your control and take appropriate measures to protect it;
- Follow labeling, handling, sharing, storage and destruction requirements based on appropriate classification / sensitivity level;
- When in doubt about the classification of specific information, ask your supervisor;
- Comply with all regulatory, business or legal data retention policies before disposing of information.

6.4 Risk Management – Requirement 12.2

Control Objective: The organization implements a risk-assessment process.

Standard: The Information Security Officer has established an information security risk assessment process, which:

(a) Is performed at least annually or upon significant changes to the environment (e.g., acquisition, merger, relocation);
(b) Is incorporated for all projects associated with the processing environment
(c) Identifies critical assets, threats, and vulnerabilities; and
(d) Includes reporting of findings to the management
(e) Includes management undertaking risk treatment decisions

6.5 Management of Service Providers – Requirement 12.8

Control Objective: The organization oversees the security of service providers with whom it shares credit card information

Standard: The Information Security Officer has established an information security risk assessment process, which, on an annual basis:

(a) Identifies the service providers who have access to credit card information
(b) Assesses the PCI compliance status of the service providers
(c) Monitors the PCI compliance of the service providers and enforces governance over the service providers by communicating risk treatment requirements

6.6 Acknowledgement to Customers – Requirement 12.9

Control Objective: The organization provides an acknowledgement to customers that it is responsible for the security of card holder information

Standard: Heggerty will ensure that it will maintain compliance with PCI DSS throughout the year. Heggerty will retain a PCI Qualified Security Auditor to validate its compliance with the PCI DSS. Heggerty will publish information about its PCI DSS compliance program on its website (www.tractorpartasap.com).

6.7 Pre-employment Screening – Requirement 12.7

Control Objective: The organization: [2]

- Screens individuals prior to authorizing access to the information system; and
- Rescreens individuals, if necessary, based on organizational concerns.

Standard: Heggerty ensures that information security best practices are incorporated into Human Resources (HR) personnel management practices. Heggerty's CEO is responsible for screening potential personnel prior to hiring in an effort to minimize the risk of compromise from internal sources. Approved methods of screening procedures include:

- Previous employment history verification;
- Criminal history record check;
- Department of Motor Vehicles (DMV) history check;
- Credit history; and
- Personal/professional reference checks.

Heggerty provides access to information with special protection measure, which is granted only to individuals who:

(a) Have signed an employment agreement
(b) Have satisfied the background screening requirements

6.8 Security Awareness Training – Requirement 12.6

Control Objective: The organization provides role-based security-related training:

- Before authorizing access to the system or performing assigned duties;
- When required by significant changes, changes in risk or changes in technology such as with development platforms; and
- At least annually thereafter.

Standard: For information security training:

Heggerty's Information Security Officer ensures initial security training is provided to personnel upon hire, and thereafter, on at least an annual basis, Methods will vary depending on the role of the personnel and their level of access to sensitive data. For end-user training:

- All users will sign an acknowledgement form stating they have read and understood Heggerty's requirements regarding information security policies, prior to having access to Heggerty information systems or data.
- All new users will attend a security awareness training within thirty (30) days of, being granted access to any information system;
- All users will at least at least one (1) hour of security awareness training at least annually.

- Application developers will obtain secure coding training at least annually as well as when the risk of the development platform changes.
- All users will be provided with sufficient training and supporting reference materials to allow them to properly protect Heggerty's information systems and data; and
- Heggerty's management will develop and maintain a communications process to be able to communicate new Information Security program information, such as an informational security bulletin or email about security items of interest.

6.9 Termination of Employment – Requirement 9.3

Control Objective: The organization, upon termination of individual employment: [3]

- Terminates information system access;
- Conducts exit interviews;
- Retrieves all security-related organizational information system-related property; and
- Retains access to organizational information and information systems formerly controlled by terminated individual.

Standard: Heggerty's management ensures that upon termination of an individual's employment:

- Information system access accounts are disabled within twenty-four (24) hours of the termination action;
- Exit interviews are conducted, if possible;
- Access to any company operated facilities is revoked such as offices, data centers or third party hosting sites;
- All company owned property is recovered; and
- All company-owned information the terminated employee was responsible for is identified and accounted for.

If a user resigns or is terminated, the following will be accomplished as soon as possible, but no longer than twenty-four (24) hours from notification of a change in a user's status:

- The user's privileges and access, logical and physical, are revoked;
- The user's passwords are changed or the accounts disabled to preclude access;
- All shared passwords known by the user on all applicable systems are changed;
- All privileged account passwords known by the user are changed;
- Incoming mail for the user will be re-directed as directed by the user's supervisor;
- After thirty (30) days, incoming mail will be disabled for the account, unless deemed necessary;
- All files owned by the user will be identified and either archived or changed to a valid user;
- All automated scripts/ batch jobs previously requested or previously submitted will be reviewed; and
- All Heggerty property will be collected, including but not limited to:
    - Keys, lock combinations and identification badges;
    - Sensitive data and documentation;
    - Operator procedures;
    - Program documentation;
    - Company-owned equipment, pagers, notebook computers and tools; and
    - Phone contact lists.

7 Data Classification and Handling

Information assets are assigned a sensitivity level based on the appropriate audience for the information. If the information has been previously classified by regulatory, legal, contractual, or company directive, then that classification will take precedence. The sensitivity level then guides the selection of protective measures to secure the information. All data are to be assigned one of the following four sensitivity levels:

Data Classification levels and handling procedures	**Restricted** (Restricted information is highly valuable, highly sensitive business information and the level of protection is dictated externally by legal and/or contractual requirements. Restricted information must be limited to only authorized employees, contractors, and business partners with a specific business need. Examples of Restricted information includes but are not limited to cardholder data, board meeting minutes, intellectual property.)	**Confidential** (Confidential information is highly valuable, sensitive business information and the level of protection is dictated internally by Heggerty. Examples of Confidential information includes but are not limited to customer lists, customer contact information, contracts, non-disclosure agreements, employee human resources information)	**Internal Use** (Internal Use information is information originated or owned by Heggerty, or entrusted to it by others. Internal Use information may be shared with authorized employees, contractors, and business partners who have a business need, but may not be released to the general public, due to the negative impact it might have on the company's business interests. Examples of Internal Use information includes but are not limited to employee names, employee email addresses, employee telephone numbers)	**Public** (Public information is information that has been approved for release to the general public and is freely shareable both internally and externally. Examples of Public information includes but are not limited to sales brochures, services marketing information)
Non-Disclosure Agreement (NDA)	▪ NDA is required prior to access by non-Heggerty employees.	▪ NDA is recommended prior to access by non-Heggerty employees.	No NDA requirements	*No NDA requirements*
Internal Network Transmission (wired & wireless)	▪ Encryption is required ▪ Instant Messaging is prohibited FTP is prohibited	▪ Encryption is recommended Instant Messaging is prohibited FTP is prohibited	*No special requirements*	*No special requirements*
External Network Transmission (wired & wireless)	▪ Encryption is required ▪ Instant Messaging is prohibited	▪ Encryption is required ▪ Instant Messaging is prohibited	▪ Encryption is recommended Instant ▪ Messaging is prohibited	*No special requirements*

	▪ FTP is prohibited ▪ Remote access should be used only when necessary and only with VPN and two-factor authentication	▪ FTP is prohibited	▪ FTP is prohibited	
Data At Rest (file servers, databases, archives, etc.)	▪ Encryption is required Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific individuals	▪ Encryption is recommended ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups	▪ Encryption is recommended ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups	▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups
Mobile Devices (iPhone, iPad, MP3 player, USB drive, etc)	▪ Encryption is required ▪ Remote wipe must be enabled, if possible	▪ Encryption is required ▪ Remote wipe must be enabled, if possible	▪ Encryption is recommended ▪ Remote wipe should be enabled, if possible	*No special requirements*
Email (with and without attachments)	▪ Encryption is required ▪ Do not forward	▪ Encryption is required ▪ Do not forward	▪ Encryption is recommended	*No special requirements*
Physical Mail	▪ Mark “Open by Addressee Only” ▪ Use “Certified Mail” and sealed, tamper-resistant envelopes for	▪ Mark “Open by Addressee Only” Use “Certified Mail” and sealed, tamper-resistant envelopes for	▪ Mail with company interoffice mail US Mail or other public delivery systems and sealed,	*No special requirements*

	external mailings ▪ Delivery confirmation is required ▪ Hand deliver internally	external mailings ▪ Delivery confirmation is required ▪ Hand delivering is recommended over interoffice mail	tamper-resistant envelopes for external mailings	
Printer	▪ Verify destination printer ▪ Attend printer while printing	▪ Verify destination printer ▪ Attend printer while printing	▪ Verify destination printer ▪ Retrieve printed material without delay	*No special requirements*
Web Sites	▪ Posting to intranet sites is prohibited, unless it is pre-approved to contain Restricted data. ▪ Posting to Internet sites is prohibited, unless it is pre-approved to contain Restricted data.	▪ Posting to publicly-accessible Internet sites is prohibited.	▪ Posting to publicly-accessible Internet sites is prohibited	*No special requirements*
Telephone	▪ Confirm participants on the call line ▪ Ensure private location	▪ Confirm participants on the call line ▪ Ensure private location	*No special requirements*	*No special requirements*

Video / Web Conference Call	▪ Pre-approve roster of attendees ▪ Confirm participants on the call line ▪ Ensure private location	▪ Pre-approve roster of attendees ▪ Confirm participants on the call line ▪ Ensure private location	▪ Pre-approve roster of attendees ▪ Confirm participants on the call line	*No special requirements*
Fax	▪ Attend receiving fax machine ▪ Verify destination number ▪ Confirm receipt ▪ Do not fax outside company without manager approval	▪ Attend receiving fax machine ▪ Verify destination number ▪ Confirm receipt ▪ Do not fax outside company without manager approval	*No special requirements*	*No special requirements*
Paper, Film/Video, Microfiche	▪ Return to owner for destruction ▪ Owner personally verifies destruction	▪ Shred or delete all documents or place in secure receptacle for future shredding	▪ Shred or delete all documents or place in secure receptacle for future shredding	*No special requirements*
Storage Media (Hard Disk Drives (HDDs), Flash drives, tapes, CDs/DVDs, etc.)	▪ Physically destroy the hard drives and media ▪ Requires use of company-approved vendor for destruction	▪ Physically destroy the hard drives and media or use commercial overwrite software to destroy the data on the media (quick reformat of	▪ Physically destroy the hard drives and media or use commercial overwrite software to destroy the data on the media	▪ Physically destroy the hard drives and media or use commercial overwrite software to destroy the data on the media

		the media is not sufficient)		

8 User Security – Requirement 7,8,12.3

Control Objective: Assigning a unique identification to each person with access ensures that each individual is uniquely accountable for their actions. When such accountability is in place, actions taken on critical data systems are performed by, and can be traced to known and authorized users and processes.

Standard:

User Provisioning: Each employee will be provided a unique User ID with associated access levels commensurate with their job functions, including remote access. The use of non-authenticated User IDs or User IDs not associated with a single identified user are prohibited. Shared or group User IDs are never permitted for user-level access. Privileged access levels are granted based on roles and to users based on business need. The Network Security Engineer is responsible for granting users access to the processing environment. Access to the processing environment is granted to the Network Security Engineer and the Information Security Officer, and to the Product Security Engineers, when required.

Configuration parameters are set for the following:

- Minimum password length = 8 characters
- Password Age = 90 days
- Password Complexity = Alpha-numeric, Special Characters
- Password reset upon first time use
- Lockout User ID after 6 repeated incorrect attempts
- Session Timeout = 15 minutes
- Lockout Duration = 30 minutes

Termination of Employment: Heggerty's management ensures that upon termination of an individual's employment:

- Information system access accounts, including remote access, are disabled within twenty-four (24) hours of the termination action;
- Exit interviews are conducted, if possible;
- Access to any company operated facilities is revoked such as offices, data centers or third party hosting sites;
- All company owned property is recovered; and
- All company-owned information the terminated employee was responsible for is identified and accounted for.

If a user resigns or is terminated, the following will be accomplished as soon as possible, but no longer than twenty-four (24) hours from notification of a change in a user's status:

- The user's privileges and access are revoked;
- The user's passwords are changed or the accounts disabled to preclude access;
- All shared passwords known by the user on all applicable systems are changed;
- All privileged account passwords known by the user are changed;
- Incoming mail for the user will be re-directed as directed by the user's supervisor;
- After thirty (30) days, incoming mail will be disabled for the account, unless deemed necessary;
- All files owned by the user will be identified and either archived or changed to a valid user;
- All automated scripts/ batch jobs previously requested or previously submitted will be reviewed; and
- All Heggerty property will be collected, including but not limited to:
    - Keys, lock combinations and identification badges;
    - Sensitive data and documentation;
    - Operator procedures;
    - Program documentation;
    - Company-owned equipment, pagers, notebook computers and tools; and
    - Phone contact lists

9 Network Security – Requirement 1,2

Control Objective: All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the internet as an e-commerce, employee internet access through desktop browser, employee email access, dedicated connections such as business-to-business connections via wireless networks, or via other sources.

Standard: Heggerty has implemented a defense in depth security architecture to protect the processing environment and associated information. Heggerty has implemented web application firewalls, which in addition to limiting access to the processing environment, also act as a source of identity for unauthorized access attempts.

9.1 IT Change Management

Heggerty has implemented a formal change management process that is used to govern changes to the processing environment. This includes making changes to the networking infrastructure (firewalls), computing infrastructure (guest operating systems) or the web applications. The following is the change management process:

1. A change requestor documents the requested change in an email and send it to the Heggerty Change Management Board
2. Heggerty's Change Management Board reviews the requested change and provides its decision to or not to make the change. Any significant changes will include a PCI review that will be conducted by the Information Security Officer.
3. If approved by the Change Management Board, the change is tested. The test results are shared with the Change Management Board, who has the final authority to approve or reject a change request

4. All records of change requests and associated decisions are retained in the Change Management Board's mailbox

9.2 Firewall Security

The Cloud Service Provider is responsible for hardening the operating system of the firewalls. Heggerty is responsible for defining the access control lists on the firewall. The following are the hardening standards

1. All firewall implementations would adopt the principle of least privilege and deny all inbound traffic by default. The ruleset would be opened incrementally to only allow permissible traffic.
2. Anti-spoofing measures are implemented
3. Network Address Translation is enabled
4. Firewall rulesets are reviewed every six months. The review is performed by the Network Security Engineer and Information Security Officer
5. The firewall ruleset configuration is backed up to Heggerty' offline storage
6. Firewalls logs are sent to the centralized log management system

10 Data Security – Requirement 3

Control Objective: Protection methods such as encryption, truncation and masking are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to the encrypted data. Without the proper cryptographic keys, the data is unreadable and unusable to that person.

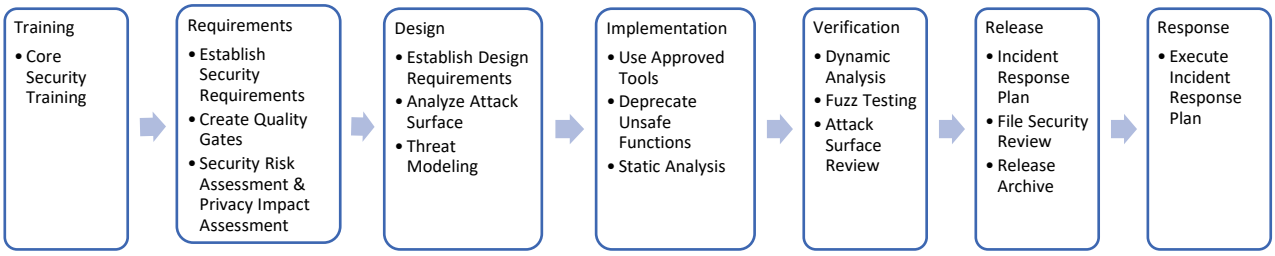
Standard: Heggerty uses a tokenization service which results in the avoidance of transmitting unencrypted cardholder data in Heggerty's processing environment. Heggerty has conducted due diligence on the vendors used for tokenization, and has defined roles and responsibilities as it relates to the security of the cardholder data.

Please refer to the data flow diagram for an overview of flow of information in the supply chain.

Data Retention : Heggerty does not retain credit card information in an unencrypted format.

11 Software Development Security – Requirement 6

Heggerty's secure software development program is based on Microsoft's Secure Development Lifecycle methodology, which is a software development process that helps developers build more secure software and address security compliance requirements while reducing development costs. The following diagram provides an overview of the various phases of Heggerty's secure software development program and their associated activities.



While this methodology has been adopted by Heggerty, it should be noted that Heggerty will be required to align its development activities with client dictated methodologies. That said, Heggerty employees will be trained in this methodology, and will be used for the following:

- All software releases – will be subject to implementation of control practices through each of the above phases of the program prior to approval of the change control documentation and/or release into the live environment;
- Third party or acquired web applications – when possible, third party of acquired web applications will be subject to an initial quality assurance check after which each will be bound to Policy requirements;
- Patch or update Releases – will be subject to quality assurance levels based on the risk of the changes to the application functionality and/or architecture; and
- Emergency releases – will be allowed to forgo security assessments and carry the assumed risk until such time that a static code analysis can be carried out. Hotfixes will be designated as such by the Product Security Coordinator or an appropriate manager who has been delegated this authority.

11.1 Training

IT Department will train all its personnel on the secure software development lifecycle and related Heggerty policy requirements. Additional trainings might include secure design and threat modelling principles. All developers will be trained on OWASP's (**the Open Web Application Security Project**) Top 10 vulnerabilities, secure coding techniques and ethical hacking of web applications. Training is based on e-learning using Heggerty's Learning Management System.

11.2 Requirements

IT Department will document security and privacy requirements for each solution. Documents will be created prior to the solution implementation planning leading up to each solution release, and included in "what to expect" document for each release. Security gates will be established and all components and features will pass the security gate for integration as part of the release criteria.

11.3 Design

For every project delivering into a release, Development will:

- Complete security questionnaire for design related security requirements for web applications (for e.g., OWASP Application Security Verification Standard)
- Define privacy requirements;
- Analyze the attack surface by running a Attack Surface Analyzer tool;
- Perform threat modelling using a threat modeling tool.

- A security gate will include the review of the threat model by Information Security.

11.4 Implementation

IT Department will implement secure coding standards that address the OWASP Top 10 vulnerabilities within a testing environment prior to migration to production.

Static code analysis will be used to validate that Development's secure coding activities are in compliance with the Policy's requirements and to identify coding flaws, backdoors and malicious code.

For new code, all errors identified during static code analysis will be remediated before migrating code to the verification phase. If legacy code is reused for a new module, static code analysis will be performed and all errors remediated, before migrating code to the verification phase.

11.5 Verification

At the conclusion of the implementation phase, IT Department will perform the following quality assurance checks for all software releases:

- Dynamic code analysis, or black-box testing to identify vulnerabilities in run time;
- Fuzz testing (e.g., OpenFuzz);

11.5.1 Third Party or Acquired Web Applications

All third party, open source or acquired web applications will be evaluated. The results of the assessment will be presented to the IT Department leadership, which will have the final authority on decisions related to the use of the third-party software.

11.6 Release

The IT Department leadership will review documentation related to the development lifecycle and will make a final determination if code can be migrated to the production environment. Additionally, for websites used to conduct eCommerce, the PCI approved scanning vendor will conduct vulnerability scans.

12 Physical Security – Requirement 9

Control Objective: Any physical access to data or systems that cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies and should be appropriately restricted.

Standard: Heggerty's processing environment is hosted in third party data centers (e.g., NetSuite and Epicor), and Heggerty's data center. Heggerty relies on independent reports (PCI DSS AOC/ROC, SSAE 18) to validate the physical security of its third-party providers. The following are physical security standards for Heggerty data centers.

12.1 Access to Heggerty Facilities

- **Employee Access:** Employee badges are created with the approval of HR. The badges are to be worn at all times in a visible location by the employee. Access changes to existing badges should be made based on an employee's role and function. If an employee requires access to

a restricted area, the employee's manager should forward an approval request, requesting that access be enabled for a specific employee.
    - At the time of employee separation, the following actions are to take place:
        - Badges are to be collected by HR or the manager of the former employee.
        - HR should notify the Office Manager to terminate access privileges assigned to the physical badge.

- **Visitor Access:** The following steps are required of visitors entering Heggerty facilities:
    - Visitors should be provided with physical badges identifying them as such.
    - Visitor badges should be displayed at all times.
    - Visitor badges should be returned to security at the end of each day.
    - Visitor badges should expire automatically.

12.2 Access to Data Center & Utilities

- **Locks:** Physical access to confidential information must be protected by one of the following methods
    - Magnetic locks & card readers
    - Standard lock and key
- **Sign-in Log:** A sign-in log of all non-employees or visitors is maintained for a minimum of 3 months by physical security within area having restricted access. Archives of the logs are maintained for a minimum of one year. The log contains the following information:
    - Time of arrival
    - Time of departure
    - Company of non-employee
    - Employee who is responsible for the visitor
    - Reason for visit
- **Use of Video Cameras:** The following practices are to be followed with respect to video cameras within data centers:
    - Video cameras must be present to monitor the entry/exit points of data centers where cardholder data is stored or present.
    - Video cameras should be installed internal to the data center or otherwise protected from tampering or disabling.
    - Video cameras should be monitored, and video feed data stored for 3 months.
- **Console Logout:** When access to workstations, servers or other consoles in the datacenter is not required, they must be locked out or the user must logout of the system. Employees who use systems within the datacenter are responsible for ensuring compliance with this practice.

12.3 Maintenance of Printed Confidential Documents

- **On-site Storage**: On-site storage of confidential physical materials (such as materials with NPI) must be secured and monitored. Periodic physical inspections of physical material inventories should be performed to document the presence of confidential physical material. A copy of this documentation should be stored by the Office Manager.

- **Off-site Storage**: All confidential hardcopy materials sent outside the facility must be documented and authorized by management. A copy of the document which tracks the confidential materials being removed is to be maintained for 1 year by the Office Manager. Off-site storage of confidential hardcopy materials is to be kept within a secured vendor facility. The vendor facility for off-site storage must enforce physically security to disallow access to backup media and should meet or exceed local fire code standards. Monthly reviews

of access to the warehouse where physical documents are maintained should be performed by the manager responsible for access to those areas.

13 Incident Response and Management – Requirement 12

Heggerty will maintain an information security incident handling capability that includes adequate preparation, detection, analysis, containment, recovery, and reporting activities.

Management Intent: The purpose of this policy is to establish and maintain a capability to guide Heggerty's response when cyber-security incidents occur. The objective is to ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses. Management responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security incidents.

13.1 Incident Response Process – Requirement 12.10

Control Objective: The organization ensures an incident response capability exists and is prepared to respond immediately to potential information security incidents.

Standard:

This Incident Response Plan describes Heggerty's protocol for responding to any information security Incident. It defines the roles and responsibilities of Heggerty's incident Response Team ("IRT"), characterization of Incidents, personal data breach notification processes, reporting requirements and its relationship to other Heggerty policies.

This Plan applies to incidents associated with any information that is collected, stored or processed by Heggerty and its subcontractors. The IRT, led by Heggerty's Information Security Officer, shall be responsible for overseeing the development, implementation, and maintenance of the plan. This plan will be reviewed and tested at least on an annual basis to ensure relevant information is appropriately considered.
The following is a high-level overview of the incident response process

The following are the steps involved in incident response:

13.1.1 Evaluation and Classification of Incidents

In order to ensure an Incident response process that assures prompt notification of senior management and the Board as dictated by the probable severity of damage and potential loss related to adverse events, the Information Security Officer will make a risk assessment on all Incident reports. In assessing the risk, the Information Security Officer will consider the following factors on a case-by-case basis:

- Type of breach (confidentiality, integrity, availability, resilience);
- Whether data is intelligible and whether any encryption key has been compromised;
- Nature, sensitivity and volume of Personal Data involved in the Incident;
- Ease of identification of consequences;
- Severity of consequences for individuals;
- Special characteristics of the individual;
- The number of affected individuals; and

In concluding the risk assessment, the Information Security Officer will categorize the Incident in accordance with the following levels of severity:

Incident Severity	Definition
Level 0: Reportable	No interruption in data processing operations All Incidents that will not affect operation of business but need to be reported to the Heggerty Management
Level 1: Low	Any security incident which has been successfully responded to and which does not have the potential, over time, to affect inherent operational or reputational risk.
Level 2: Medium	Any security Incident where it is clear that a person has been specifically targeting Heggerty for the purpose of breaching security.
Level 3: High	Any security Incident where it is clear that the attacker has breached the security of systems. Any event that may increase reputational or legal risk if not addressed immediately.
Level 4: Critical	Any security Incident in which protected customer information has been breached. The Information Security Officer determines that the IRT must consider involving law enforcement.

13.1.2 Remedial Action and Analysis

At the Information Security Officer's discretion, based on the type of Incident, the actual response to an event will fall into the general categories of containment, eradication, recovery, and follow-up. Response usually occurs concurrently with overview, evaluation, and notification.

The Information Security Officer is responsible for managing and collecting forensic evidence. The following rules will be followed:

- No forensic evidence may be damaged, destroyed or otherwise compromised by the procedures used during the investigation.
- Investigation is not performed directly on the evidence. Evidence is imaged using forensic techniques.
- A chain of custody must be established and maintained.
- The Information Security Officer has the authority to hire and/or retain a third party to collect forensics data so that independence is established and there is no appearance of a conflict of interest.

Definition of Critical Logs and Events

The following are examples of critical events that Heggerty will review as part of the forensic investigation of system logs:

- Account Management – Success / Failure
- System Events – Success / Failure
- Directory Service Access – Success / Failure
- Active Directory Object Access Attempts – Success / Failure
- Active Directory Object Deletions

- Group Policy Management
- User account changes that provide administrator equivalent permissions.
- Changes to Groups --- adds, changes, or deletions.
- Password Reset Attempts by Users
- Password Reset Attempts by Administrators or Account Operations
- Login Events – Success / Failure
- Disk Capacity Failures
- Manual changes to the registry – add, changes, and deletions.
- AVS Application Update errors
- AVS DAT Update Errors
- Unexpected Server reboots
- Access to Network Infrastructure
- Changes to ACLs on switches, routers, or firewalls
- Windows Update Failures
- Licensing Errors
- Hardware Errors
- Backup Errors
- DNS Errors

13.2 Incident Response Testing and Training - Requirement 12.10.2

Control Objective: The organization:

- Trains personnel in their incident response roles and responsibilities with respect to information systems; and
- Provides refresher training.

Standard: On at least an annual basis, the Information Security Officer tests the incident response plan by conducting tabletop exercises.

13.3 Incident Reporting - Requirement 12.8.3

Control Objective: The organization:

- Requires personnel to report suspected security incidents to organizational incident response personnel within organization-defined time-periods; and
- Reports security incident information to designated authorities.

Standard: Employees and contractors using Heggerty's information systems and services will be required to note and report any observed or suspected information security weaknesses in systems or services. Heggerty requires its workforce to report all security incidents to the Information Security Officer. Documenting information system security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information will be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

14 Security Logging – Requirement 10.1 to 10.5.5

Control Objective: Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting and analysis when something goes wrong.

Standard: All systems will create security logs when the following events occur:

- Create, read, update, or delete Confidential Information, including confidential authentication information such as passwords;
- Create, update, or delete information not covered in #1 above;
- Initiate a network connection;
- Accept a network connection;
- User authentication and authorization for activities covered in #1 or #2 above, such as user login and logout;
- Grant, modify, or revoke access rights, including adding a new user or group, changing user privilege levels, changing file permissions, changing database object permissions, changing firewall rules, and user password changes;
- System, network, or services configuration changes, including installation of software patches and updates, or other installed software changes;
- Application process startup, shutdown, or restart;
- Application process abort, failure, or abnormal end, especially due to resource exhaustion or reaching a resource limit or threshold (such as for CPU, memory, network connections, network bandwidth, disk space, or other resources), the failure of network services such as DHCP or DNS, or hardware fault; and
- Detection of suspicious/malicious activity such as from a firewall, intrusion detection system, anti-virus system, or anti-spyware system.

Such logs shall identify or contain at least the following elements, directly or indirectly. In this context, the term “indirectly” means unambiguously inferred.

- **Type of action** – examples include authorize, create, read, update, delete, and accept network connection.
- **Subsystem performing the action** – examples include process or transaction name, process or transaction identifier.
- **Identifiers (as many as available) for the subject requesting the action** – examples include username, computer name, IP address, and MAC address. Note that such identifiers should be standardized in order to facilitate log correlation.
- **Identifiers (as many as available) for the object the action was performed on** – examples include file names accessed, unique identifiers of records accessed in a database, query parameters used to determine records accessed in a database, computer name, IP address, and MAC address. Note that such identifiers should be standardized in order to facilitate log correlation.
- **Before and after values** when action involves updating a data element, if feasible.
- **Date and time the action was performed**, including relevant time-zone information if not in Coordinated Universal Time.
- **Whether the action was allowed or denied** by access-control mechanisms.
- **Description and/or reason-codes** of why the action was denied by the access-control mechanism, if applicable.

Time Settings: All Heggerty managed devices will be configured to use synchronized time sources (i.e., Network Time Protocol - NTP) such that the times on these devices are sync to the common time source on a regular basis so that time stamps across all the logs are consistent.

Security of Logs: Security logs will be protected against unauthorized modification. Only Heggerty's Information Security Officer and Network Security Engineer(s) will have access to the logs. In addition to protecting the logs from unauthorized access, Heggerty ensures the integrity of the logs through automated file integrity management tools.

Log Retention: Logs are retained online for at least 30 days and offline for at least 12 months. Due to storage or technical constraints, some logs will not fit in the initial log reporting system. In these cases, logs are moved to another storage environment, but must still be retrievable for analysis throughout the defined retention period

15 Security Monitoring – Requirement 10.6 to 10.9

Control Objective: Without continuous monitoring, an occurrence of unauthorized access cannot be detected in a timely manner.

Standard: Automated tools will provide real time notification of detected wrongdoing and vulnerability exploitation. Where possible a security baseline will be developed, and the tools will report exceptions. These tools will be deployed to monitor:

- Internet traffic;
- LAN traffic, protocols, and device inventory; and
- Operating system security parameters.

The following files will be checked for signs of wrongdoing and vulnerability exploitation on a daily basis:

- Automated intrusion detection system logs;
- Firewall logs;
- User account logs;
- Network scanning logs;
- Operating System logs;
- Application logs;
- File Integrity Manager

All security issues discovered will be reported to Heggerty's Information Security Officer and will be investigated per Heggerty's Incident Response process.

16 Vulnerability Management – Requirements 5,11

Control Objective: Vulnerabilities are being discovered continually by malicious individuals and researchers and being introduced by a new system. System components and custom software should be tested to ensure security controls continue to reflect a changing environment.

Standard: Heggerty will install anti-virus solutions and host intrusion detection solutions on all systems in the processing environment. The tools will be used to proactively detect threats and vulnerabilities in the processing environment.

Additionally, Heggerty has retained a PCI Approved Scanning Vendor (ASV) to conduct internal and external network and web application vulnerability scans. The vulnerability scans will be conducted on a

monthly basis. Additionally, Heggerty has retained an ASV to conduct internal and external penetration testing of the processing environment. The Information Security Officer, in collaboration with the Network and Product Security Engineers, will conduct a risk assessment of the reported vulnerability. All vulnerabilities will be remediated per the service level agreements detailed in the table below.

Servers will comply with the minimum baseline requirements that have been approved by Heggerty's Information Security Officer. These minimum baseline requirements define the default operating system level, service pack, hotfix, and patch level required to ensure the security of the Heggerty asset and the data that resides on the system.

Network Security Engineer will maintain and report metrics that summarize the outcome of each patching cycle. These reports shall be used to evaluate the current patching levels of all systems and to assess the current level of risk. These reports shall be made available to the Information Security Officer upon request.

CVSS Rating	Severity Level	Internal Scan Results	External Scan Results
7.0-10.0	High	Fail	Fail
4.0-6.9	Medium	Pass	Fail
0.0-3.9	Low	Pass	Pass

In the event that a risk cannot be remediated based on a hardware, operating system, or software (for example, a legacy application that has no upgrade), any deficiency, will need to be mitigated and approved (as an exception based on acceptance of the risk) by the Heggerty Information Security Officer and added to Heggerty's risk register for tracking and assessment purposes. This risk register will be reviewed by the Information Security Officer on a quarterly basis to ensure the risk acceptance is still justified.

To ensure the integrity of the systems used in the processing environment, Heggerty has implemented a file integrity manager to detect unauthorized changes to critical operating system files. The alerts generated by the file integrity manager are collected in the centralized log management solution and reviewed by Heggerty's Network Security Engineer.