Version 2.0 Agreement Approved: June 2019

DATA PRIVACY AGREEMENT (DPA)
FOR TEXAS K-12 INSTITUTIONS

Lackland ISD 10/22/2020

LEA NAME [Box 1] DATE [Box 2]

and

Charmtech Labs LLC 10/21/2020

OPERATOR NAME [Box 3] DATE [Box 4]

Background and Instructions

History of Agreement- This agreement has been drafted by the Texas Student Privacy Alliance (TXSPA). The Alliance is a collaborative group of Texas school districts that share common concerns around student and data privacy. The Texas K-12 CTO Council is the organization that sponsors the TXSPA and the TXSPA is the Texas affiliate of the national Student Data Privacy Consortium (SDPC). The SDPC works with other state alliances by helping establish common data privacy agreements unique to the jurisdiction of each state. This Texas agreement was drafted specifically for K-12 education institutions and included broad stakeholder input from Texas school districts, statewide associations such as TASB, TASA, and TASBO, and the Texas Education Agency. The purpose of this agreement is to set standards of both practice and expectations around data privacy such that all parties involved have a common understanding of expectations. This agreement also provides a mechanism (Exhibit E- General Offer of Terms) that would allow an Operator to extend the ability of other Texas school districts to be covered under the terms of the agreement should an Operator sign Exhibit E. This mechanism is intended to create efficiencies for both Operators and LEAs and generally enhance privacy practices and expectations for K-12 institutions and for companies providing services to K-12 institutions.

Instructions for Operators: This agreement is intended to be provided to an Operator from a LEA. The Operator should fully read the agreement and is requested to complete the below areas of the agreement. Once the Operator accepts the terms of the agreement, the Operator should wet sign the agreement and return it to the LEA. Once the LEA signs the agreement, the LEA should provide a signed copy of the agreement to the Operator.

Article/Exhibit	Box #	Description
Cover Page	Box # 3	Official Name of Operator
Cover Page	Box # 4	Date Signed by Operator
Recitals	Box #5	Contract Title for Service Agreement
Recitals	Box #6	Date of Service Agreement
Article 7	Boxes #7-10	Operator's designated representative
Signature Page	Boxes #15-19	Authorized Operator's representative signature
Exhibit A	Box #25	Description of services provided
Exhibit B	All Applicable Boxes	• Operator notates if data is collected to provide the described services. • Defines the schedule of data required for the Operator to provide the services outlined in Exhibit A
Exhibit D	All Applicable Boxes	(Optional Exhibit): Defines deletion or return of data expectations by LEA

Exhibit E	All Applicable Boxes	(Optional Exhibit): Operator may, by signing the Form of General Offer of Privacy Terms (General Offer, attached as Exhibit E), be bound by the terms of this DPA to any other Subscribing LEA who signs the acceptance in said Exhibit.
Exhibit F	Boxes # 25-29	A list of all Subprocessors used by the Operator to perform functions pursuant to the Service Agreement, list security programs and measures, list Operator's security measures

Instructions for LEA and/or Subscribing LEA: This agreement is intended to be provided to an Operator from a LEA. Upon receiving an executed agreement from an Operator, the LEA should fully review the agreement and if agreeable, should have an authorized LEA contact wet sign the agreement. Once signed by both the Operator and LEA, the LEA should send a copy of the signed agreement to the Operator.

Article/Exhibit	Box #	Description
Cover Page	Box # 1	Official Name of LEA
Cover Page	Box #2	Date Signed by LEA
Article 7	Boxes #11-14	LEA's designated representative
Signature Page	Boxes #20-24	Authorized LEA representative's signature
Exhibit D	All Applicable Boxes	(Optional Exhibit): Defines deletion or return of data expectations by LEA
Exhibit E	All Applicable Boxes	(Optional Exhibit) Only to be completed by a Subscribing LEA

RECITALS

WHEREAS, the Operator has agreed to provide the Local Education Agency (“LEA”) with certain digital educational services (“Services”) according to a contract titled “harmtech Labs service agreemer“
[Box 5]
and dated 10/21/202 (tbe “Service Agreement”), and
[Box 6]

WHEREAS, in order to provide the Services described in the Service Agreement, the Operator may

receive or create and the LEA may provide documents or data that are covered by federal statutes, among them, the Federal Educational Rights and Privacy Act (“FERPA”) at 20 U.S.C. 1232g (34 CFR Part 99), Children’s Online Privacy Protection Act (“COPPA”), 15 U.S.C. 6501-6506, and Protection of Pupil Rights Amendment (“PPRA”) 20 U.S.C. 1232h; and

WHEREAS, the documents and data transferred from LEAs and created by the Operator’s Services are also subject to state student privacy laws, including Texas Education Code Chapter 32; and

WHEREAS, the Operator may, by signing the "General Offer of Privacy Terms", agree to allow other

LEAs in Texas the opportunity to accept and enjoy the benefits of this DPA for the Services described within, without the need to negotiate terms in a separate DPA.

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

ARTICLE I: PURPOSE AND SCOPE

1. **Nature of Services Provided.** The Operator has agreed to provide digital educational services as outlined in Exhibit A and the Agreement.

2. **Purpose of DPA**. For Operator to provide services to the LEA it may become necessary for the LEA to share certain LEA Data. This DPA describes the Parties’ responsibilities to protect Data.

3. **Data to Be Provided**. In order for the Operator to perform the Services described in the Service Agreement, LEA shall provide the categories of data described in the Schedule of Data, attached as Exhibit B.

4. **DPA Definitions**. The definitions of terms used in this DPA are found in Exhibit C. In the event of a conflict, definitions used in this DPA shall prevail over terms used in the Service Agreement.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Ownership of Data**. All Data transmitted to the Operator pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Operator further acknowledges and agrees that all copies of such Data transmitted to the Operator, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Data contemplated per the Service Agreement shall remain the exclusive property of the LEA.

2. **Operator Materials**. Operator retains all right, title and interest in and to any and all of Operator's software, materials, tools, forms, documentation, training and implementation materials and intellectual property ("Operator Materials"). Operator grants to the LEA a personal, nonexclusive license to use the Operator Materials for its own non-commercial, incidental use as set forth in the Service Agreement. Operator represents that it has all intellectual property rights necessary to enter into and perform its obligations in this DPA and the Service Agreement, warrants to the District that the District will have use of any intellectual property contemplated by the Service Agreement free and clear of claims of any nature by any third Party including, without limitation, copyright or patent infringement claims, and agrees to indemnify the District for any related claims.

3. **Parent Access**. LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Data on the pupil's records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. Operator shall respond in a reasonably timely manner (and no later than 28 days from the date of the request) to the LEA's request for Data in a pupil's records held by the Operator to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Operator to review any of the Data accessed pursuant to the Services, the Operator shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

4. **Data Portability**. Operator shall, at the request of the LEA, make Data available including Pupil Generated Content in a readily accessible format.

5. **Third Party Request**. Should a Third Party, including law enforcement or a government entity, contact Operator with a request for data held by the Operator pursuant to the Services, the Operator shall immediately (within 1 business day), and to the extent legally permitted, redirect the Third Party to request the data directly from the LEA, notify the LEA of the request, and provide a copy of the request to the LEA. Furthermore, if legally permissible, Operator shall promptly notify the LEA of a subpoena compelling disclosure to a Third Party and provide a copy of the subpoena with sufficient time for the LEA to raise objections to the subpoena. The Operator will not use, disclose, compile, transfer, or sell the Data and/or any portion thereof to any third party or other entity or allow any other third party or other entity to use, disclose, compile, transfer or sell the Data and/or any portion thereof. Notwithstanding any provision of this DPA or Service Agreement to the contrary, Operator understands that the LEA is subject to and will comply with the Texas Public Information Act (Chapter 552, Texas Government Code). Operator understands and agrees that information, documentation and other material in connection with the DPA and Service Agreement may be subject to public disclosure.

6. **No Unauthorized Use**. Operator shall use Data only for the purpose of fulfilling its duties and obligations under the Service Agreement and will not share Data with or disclose it to any Third Party without the prior written consent of the LEA, except as required by law or to fulfill its duties and obligations under the Service Agreement.

7. **Subprocessors**. All Subprocessors used by the Operator to perform functions pursuant to the Service Agreement shall be identified in Exhibit F. Operator shall either (1) enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, such that the Subprocessors agree to protect Data in a manner the same as or better than as provided pursuant to the terms of this DPA, or (2) indemnify and hold harmless the LEA, its officers, agents, and employees from any and all claims, losses, suits, or liability including attorneys' fees for damages or costs resulting from the acts or omissions of its Subprocessors. Operator shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this DPA. Supbrocessors shall agree to the provisions of the DPA regarding governing law, venue, and jurisdition.

ARTICLE III: DUTIES OF LEA

1. **Provide Data In Compliance With State and Federal Law**. LEA shall provide data for the purposes of the Service Agreement in compliance with FERPA, COPPA, PPRA, Texas Education Code Chapter 32, and all other Texas privacy statutes cited in this DPA as these laws and regulations apply to the contracted services. The LEA shall not be required to provide Data in violation of applicable laws. Operator may not require LEA or users to waive rights under applicable laws in connection with use of the Services.

2. **Consider Operator as School Official.** The Parties agree that Operator is a "school official" under FERPA and has a legitimate educational interest in personally identifiable information from education records. For purposes of the Service Agreement and this DPA, Operator: (1) provides a service or function for which the LEA would otherwise use employees; (2) is under the direct control of the LEA with respect to the use and maintenance of education records; and (3) is subject to the requirements of FERPA governing the use and redisclosure of personally identifiable information from education records

3. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted data.

4. **Unauthorized Access Notification**. LEA shall notify Operator promptly of any known unauthorized access. LEA will assist Operator in any efforts by Operator to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF OPERATOR

1. **Privacy Compliance**. Operator may receive Personally Identifiable Information ("PII") from the District in the course of fulfilling its duties and obligations under the Service Agreement. The Operator shall comply with all applicable State and Federal laws and regulations pertaining to data privacy and security including FERPA, COPPA, PPRA, Texas Education Code Chapter 32, and all other Texas privacy statutes cited in this DPA.

2. **Employee Obligation**. Operator shall require all employees and agents who have access to Data to comply with all applicable provisions of this DPA with respect to the data shared under the Service Agreement. Operator agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Data pursuant to the Service Agreement.

3. **De-identified Information**. De-identified Information may be used by the Operator only for the purposes of development, product improvement, to demonstrate or market product effectiveness, or research as any other member of the public or party would be able to use de-identified data pursuant to 34 CFR 99.31(b). Operator agrees not to attempt to re-identify De-identified Information and not to transfer De-identified Information to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to LEA who has provided prior written consent for such transfer. Operator shall not copy, reproduce or transmit any De-identified Information or other Data obtained under the Service Agreement except as necessary to fulfill the Service Agreement.

4. **Access To, Return, and Disposition of Data**. Upon written request of LEA, Operator shall dispose of or delete all Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained, and transfer said data to LEA or LEA's designee within sixty (60) days of the date of termination and according to a schedule and procedure as the Parties may reasonably agree. Operator acknowledges LEA's obligations regarding retention of governmental data, and shall not destroy Data except as permitted by LEA. Nothing in the Service Agreement shall authorize Operator to maintain Data obtained under the Service Agreement beyond the time period reasonably needed to complete the disposition. Disposition shall include (1) the shredding of any hard copies of any Data; (2) Data Destruction; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable. Operator shall provide written notification to LEA when the Data has been disposed of.

The duty to dispose of Data shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of the DPA. The LEA may employ a "Request for Return or Deletion of Data" FORM, a sample of this form is attached on Exhibit "D"). Upon receipt of a request from the LEA, the Operator will immediately provide the LEA with any specified portion of the Data within five (5) business days of receipt of said request.

5. **Targeted Advertising Prohibition**. Operator is prohibited from using or selling Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising, or other commercial efforts by a Operator; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Data for the development of commercial products or services, other than as necessary to provide the Service to LEA. This section does not prohibit Operator from generating legitimate personalized learning recommendations.

6. **Access to Data**. Operator shall make Data in the possession of the Operator available tothe LEA within five (5) business days of a request by the LEA.

ARTICLE V: DATA PROVISIONS

1. **Data Security**. The Operator agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Operator are set forth below. Operator shall further detail its security programs and measures in Exhibit F. These measures shall include, but are not limited to:

   a. **Passwords and Employee Access**. Operator shall secure usernames, passwords, and any other means of gaining access to the Services or to Data, at a level consistent with an industry standard agreed upon by LEA (e.g. suggested by Article 4.3 of NIST 800-63-3). Operator shall only provide access to Data to employees or subprocessors that are performing the Services. Employees with access to Data shall have signed confidentiality agreements regarding said Data. All employees with access to Data shall pass criminal background checks.

   b. **Security Protocols**. Both parties agree to maintain security protocols that meet industry best practices in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Operator shall maintain all data obtained or generated pursuant to the Service Agreement in a secure computerenvironment.

   c. **Employee Training**. The Operator shall provide periodic security training to those of its employees who operate or have access to the system.

   d. **Security Technology**. When the Services are accessed using a supported web browser, Secure Socket Layer ("SSL") or equivalent technology shall be employed to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Operator shall host data pursuant to the Service Agreement in an environment using a firewall that is periodically updated according to industry standards.

   e. **Security Contact.** Operator shall provide the name and contact information of Operator's Security Contact on Exhibit F. The LEA may direct security concerns or questions to the Security Contact.

   f. **Periodic Risk Assessment.** Operator shall conduct periodic isk assessments and remediate any identified security and privacy vulnerabilities in a timely manner. Upon request, Operator will provide the LEA an executive summary of the risk assessment or equivalent report and confirmation of remediation.

g. **Backups.** Operator agrees to maintain backup copies, backed up at least daily, of Data in case of Operator's system failure or any other unforeseen event resulting in loss of any portion of Data.

h. **Audits.** Within 30 days of receiving **a** request from the LEA, and not to exceed one request per year, the LEA may audit the measures outlined in the DPA. The Operator will cooperate fully with the LEA and any local, state, or federal agency with oversight authority/jurisdiction in connection with any audit or investigation of the Operator and/or delivery of Services to students and/or LEA, and shall provide full access to the Operator's facilities, staff, agents and LEA's Data and all records pertaining to the Operator, LEA and delivery of Services to the Operator. Failure to cooperate shall be deemed a material breach of the DPA. The LEA may request an additional audit if a material concern is identified.

i. **Incident Response.** Operator shall have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of any portion of Data, including PII, and agrees to provide LEA, upon request, an executive summary of the written incident response plan.

2. **Data Breach**. When Operator reasonably suspects and/or becomes aware of an unauthorized disclosure or security breach concerning any Data covered by this Agreement, Operator shall notify the District within 24 hours. The Operator shall take immediate steps to limit and mitigate the damage of such security breach to the greatest extent possible. If the incident involves criminal intent, then the Operator will follow direction from the Law Enforcement Agencies involved in the case.

a. The security breach notification to the LEA shall be written in plain language, and address the following

1. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
2. A description of the circumstances surrounding the disclosure or breach, including the actual or estimated, time and date of the breach, and Whether the notification was delayed as a result of a law enforcement investigation.

b. Operator agrees to adhere to all requirements in applicable state and federal law with respect to a Data breach or disclosure, including any required responsibilities and procedures for notification or mitigation

c. In the event of a breach or unauthorized disclosure, the Operator shall cooperate fully with the LEA, including, but not limited to providing appropriate notification to individuals impacted by the breach or disclosure. Operator will reimburse the LEA in full for all costs incurred by the LEA in investigation and remediation of any Security Breach caused in whole or in part by Operator or Operator's subprocessors, including but not limited to costs of providing notification and providing one year's credit monitoring to affected individuals if PII exposed during the breach could be used to commit financial identity theft.

d. The LEA may immediately terminate the Service Agreement if the LEA determines the Operator has breached a material term of this DPA.

e. The Operator's obligations under Section 7 shall survive termination of this DPA and Service Agreement until all Data has been returned and/or Securely Destroyed.

ARTICLE VI- GENERAL OFFER OF PRIVACYTERMS

1. **General Offer of Privacy Terms.** Operator may, by signing the attached Form of General Offer of Privacy Terms (General Offer, attached as Exhibit E), be bound by the terms of this DPA to any other LEA who signs the acceptance in said Exhibit.

ARTICLE VII: MISCELLANEOUS

1. **Term**. The Operator shall be bound by this DPA for the duration of the Service Agreement or so long as the Operator maintains any Data. Notwithstanding the foregoing, Operator agrees to be bound by the terms and obligations of this DPA for no less than three (3) years.

2. **Termination**. In the event that either party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated.

3. **Effect of Termination Survival**. If the Service Agreement is terminated, the Operator shall dispose of all of LEA's Data pursuant to Article IV, section 5.

4. **Priority of Agreements**. This DPA shall govern the treatment of Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes cited in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, or with any other bid/RFP, license agreement, terms of service, privacy policy, or other writing, the terms of this DPA shall apply and take precedence. Except as described in this paragraph, all other provisions of the Service Agreement shall remain in effect.

5. **Notice**. All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, facsimile or e-mail transmission (if contact information is provided for the specific mode of delivery), or first-class mail, postage prepaid, sent to the designated representatives before: The designated representative for the Operator for this Agreement is:

First Name: Yury [Box 7]

Last Name: Puzis [Box 8]

Operator's Company Name: Charmtech Labs LLC [Box 9]

Title of Representative: COO [Box 10]

The designated representative for the LEA for this Agreement is:

First Name: Kyle [Box 11]

Last Name: Jones [Box 12]

LEA's Name: Lackland ISD [Box 13]

Title of Representative: Director of Technology [Box 14]

6. **Entire Agreement**. This DPA constitutes the entire agreement of the parties relating to the subject matter and supersedes all prior communications, representations, or agreements, oral or written, by the Parties. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both parties. Neither failure nor delay on the part of any party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

7. **Severability**. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

8. **Governing Law; Venue and Jurisdiction**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF TEXAS, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY IN WHICH THIS AGREEMENT IS FORMED FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.

9. **Authority**. Operator represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Data and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the Data and portion thereof is stored, maintained or used in any way.

10. **Waiver**. Waiver by any party to this DPA of any breach of any provision of this DPA or warranty of representation set forth herein shall not be construed as a waiver of any subsequent breach of the same or any other provision. The failure to exercise any right under this DPA shall not operate as a waiver of such right. All rights and remedies provided for in this DPA are cumulative. Nothing in this DPA shall be construed as a waiver or relinquishment of any governmental immunities or defenses on behalf of the LEA, its trustees, officers, employees, and agents as a result of the execution of this DPA or performance of the functions or obligations described herein.

11. **Assignment**. The Parties may not assign their rights, duties, or obligations under this DPA, either in whole or in part, without the prior written consent of the other Party except that either party may assign any of its rights and obligations under this DPA without consent in connection with any merger (including without limitation by operation of law), consolidation, reorganization, or sale of all or substantially all of its related assets or similar transaction. This DPA inures to the benefit of and shall be binding on the Parties' permitted assignees, transferees and successors.

[*Signature Page Follows*]

IN WITNESS WHEREOF, the parties have executed this DATA PRIVACY AGREEMENT FOR TEXAS K-12 INSTITUTIONS as of the last day noted below.

Operator's Representative:

BY: ______________________ [Box 15] Date: 10/21/2020 [Box 16]

Printed Name: Yury Puzis [Box 17] Title/Position: COO [Box 18]

Address for Notice Purposes: 77 Goodell St. Buffalo, NY, 14203 [Box 19]

LEA's Representative

BY: Burnie Roper [Box 20] Date: 10-22-2020 [Box 21]

Printed Name: Dr. Burnie Roper [Box 22] Title/Position: Superintendent [Box 23]

Address for Notice Purposes: 2460 Kenly Ave, Building 8265 [Box 24]

Note: Electronic signature not permitted.

EXHIBIT "A"

DESCRIPTION OF SERVICES

Description : [Box 25]
Reading diagnostics, supports, accommodations, text to speech.

EXHIBIT " B"

SCHEDULE OF DATA

Instructions: Operator should identify if LEA data is collected to provide the described services. If LEA data is collected to provide the described services, check the boxes indicating the data type collected. If there is data collected that is not listed, use the "Other" category to list the data collected.

□ We do not collect LEA Data to provide the described services.

□ We do collect LEA Data to provide the described services.

SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	☒
	Other application technology meta data-Please specify:	□
Application Use Statistics	Meta data on user interaction with application- Please specify: Logins	☒
Assessment	Standardized test scores	□
	Observation data	□
	Other assessment data-Please specify:	□
Attendance	Student school (daily) attendance data	□
	Student class attendance data	□
Communications	Online communications that are captured (emails, blog entries)	□
Conduct	Conduct or behavioral data	□
	Date of Birth	□

	Demographics	Place of Birth	□
		Gender	☒
		Ethnicity or race	□
		Language information (native, preferred or primary language spoken by student)	☒
		Other demographic information-Please specify:	□
	Enrollment	Student school enrollment	□
		Student grade level	☒
		Homeroom	□
		Guidance counselor	□
		Specific curriculum programs	□
		Year of graduation	□
		Other enrollment information-Please specify:	□
	Parent/Guardian Contact Information	Address	□
		Email	□
		Phone	□
	Parent/Guardian ID	Parent ID number (created to link parents to students)	☒
	Parent/Guardian Name	First and/or Last	☒
	Schedule	Student scheduled courses	□
		Teacher names	□
	Special Indicator	English language learner information	☒
		Low income status	□
		Medical alerts /health data	□
		Student disability information	☒
		Specialized education services (IEP or 504)	☒
		Living situations (homeless/foster care)	□
		Other indicator information-Please specify:	□

Category of Data	Elements	Check if used by your system
Student Contact Information	Address	□
	Email	☒
	Phone	□
Student Identifiers	Local (School district) ID number	☒
	State ID number	□
	Vendor/App assigned student ID number	☒
	Student app username	☒
	Student app passwords	☒
Student Name	First and/or Last	☒
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	☒
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	□
Student Survey Responses	Student responses to surveys or questionnaires	□
Student work	Student generated content; writing, pictures etc.	☒
	Other student work data -Please specify:	□
Transcript	Student course grades	□
	Student course data	□
	Student course grades/performance scores	□
	Other transcript data -Please specify:	□
	Student bus assignment	□
	Student pick up and/or drop off location	□

	Transportation	Student bus card ID number	□
		Other transportation data -Please specify:	□
	Other	Please list each additional data element used, stored or collected through the services defined in Exhibit A	□

EXHIBIT "C"

DEFINITIONS

HB 2087: The statutory designation for what is now Texas Education Code Chapter 32 relating to pupil records.

Data: Data shall include, but is not limited to, the following: student data, educational records, employee data, metadata, user content, course content, materials, and any and all data and information that the District (or any authorized end user(s)) uploads or enters through their use of the product. Data also specifically includes all personally identifiable information in education records, directory data, and other non-public information for the purposes of Texas and Federal laws and regulations. Data as specified in Exhibit B is confirmed to be collected or processed by the Operator pursuant to the Services. Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Operator's services.

De-Identified Information (DII): De-Identified Information is Data subjected to a process by which any Personally Identifiable Information ("PII") is removed or obscured in a way that eliminates the risk of disclosure of the identity of the individual or information about them, and cannot be reasonably re-identified.

Data Destruction: Provider shall certify to the District in writing that all copies of the Data stored in any manner by Provider have been returned to the District and permanently erased or destroyed using industry best practices to assure complete and permanent erasure or destruction. These industry best practices include, but are not limited to, ensuring that all files are completely overwritten and are unrecoverable. Industry best practices do not include simple file deletions or media high level formatting operations.

NIST 800-63-3: Draft National Institute of Standards and Technology ("NIST") Special Publication 800-63-3 Digital Authentication Guideline.

Personally Identifiable Information (PII): The terms "Personally Identifiable Information" or "PII" shall include, but are not limited to, Data, metadata, and user or pupil-generated content obtained by reason of the use of Operator's software, website, service, or app, including mobile apps, whether gathered by Operator or provided by LEA or its users, students, or students' parents/guardians. PII includes Indirect Identifiers, which is any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty. For purposes of this DPA, Personally Identifiable Information shall include the categories of information listed in the definition of Data.

Pupil-Generated Content: The term "pupil-generated content" means materials or content created by a pupil during and for the purpose of education including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of pupil content.

Subscribing LEA: A LEA that was not party to the original Services Agreement and who accepts the Operator's General Offer of Privacy Terms.

Subprocessor: For the purposes of this Agreement, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Operator, who Operator uses for data collection, analytics, storage, or other service to operate and/or improve its software, and who has access to PII.

Targeted Advertising: Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student generated content or inferred over time from the usage of the Operator's website, online service or mobile application by such student or the retention of such student's online activities or requests over time.

Texas Student Privacy Alliance: The Texas Student Privacy Alliance (TXSPA) is a collaborative group of Texas school districts that share common concerns around student privacy. The goal of the TXSPA is to set standards of both practice and expectations around student privacy such that all parties involved have a common understanding of expectations. The Texas K-12 CTO Council is the organization that sponsors TXSPA and the TXSPA is the Texas affiliate of the National Student Privacy Consortium.

EXHIBIT "D"

SAMPLE REQUEST FOR RETURN OR DELETION OF DATA

Instructions: This Exhibit is optional and provided as a sample ONLY. It is intended to provide a LEA an example of what could be used to request a return or deletion of data.

____ directs____ to
LEA OPERATOR

dispose of
return

data obtained by Operator pursuant to the terms of the Service Agreement between LEA and Operator. The terms of the Disposition are set forth below:

1. Extent of Return or Disposition

□ Return or Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

□ Return or Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Return or Disposition

□ Disposition shall be by destruction or deletion of data.

□ Return shall be by a transfer of data. The data shall be transferred to the following site as follows:

3. **Timing of Return or Disposition**

Data shall be returned or disposed of by the following date:

□ As soon as commercially practicable

□ By the following agreed upon date:

4. **Signatures**

____________________________________ ____________________

Authorized Representative of LEA Date:

5. **Verification of Disposition of Data**

____________________________________ ____________________

Authorized Representative of Operator Date:

EXHIBIT “ E”

GENERAL OFFER OF PRIVACY TERMS

Instructions: This is an optional Exhibit in which the Operator may, by signing this Exhibit, be bound by the terms of this DPA to any other Subscribing LEAs who sign the acceptance in said Exhibit. The originating LEA SHOULD NOT sign this Exhibit, but should make Exhibit E, if signed by an Operator, readily available to other Texas K-12 institutions through the TXSPA web portal. Should a Subscribing LEA, after signing a separate Service Agreement with Operator, want to accept the General Offer of Terms, the Subscribing LEA should counter-sign the Exhibit E and notify the Operator that the General Offer of Terms have been accepted by a Subscribing LEA.

1. Offer of Terms

Operator offers the same privacy protections found in this DPA between it and Lackland Independent School District and which is dated [10/21/2020] to any other LEA (“Subscribing LEA”) who accepts this General Offer through its signature below. This General Offer shall extend only to privacy protections and Operator’s signature shall not necessarily bind Operator to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Operator and the other LEA may also agree to change the data provided by LEA to the Operator to suit the unique needs of the LEA. The Operator may withdraw the General Offer in the event of:

(1) a material change in the applicable privacy statutes;
(2) a material change in the services and products listed in the Originating Service Agreement;
(3) the expiration of three years after the date of Operator’s signature to this Form.

Operator shall notify the Texas Student Privacy Alliance (TXSPA) in the event of any withdrawal so that this information may be may be transmitted to the Alliance’s users.

Operator’s Representative:

BY:

Date: 10/23/2020

Printed Name: Yury Puzis

Title/Position: COO

2. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Operator, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and Operator shall therefore be bound by the same terms of this DPA. The Subscribing LEA, also by its signature below, agrees to notify Operator that it has accepted this General Offer, and that such General Offer is not effective until Operator has received said notification.

Subscribing LEA’s Representative:

BY:

Date:

Printed Name:

Title/Position:

EXHIBIT "F"

DATA SECURITY

1. **Operator's Security Contact Information:**

Yury Puzis
____ [Box 26]
Named Security Contact

yury@team.captivoice.com
____ [Box 27]
Email of Security Contact

____ [Box 28]
Phone Number of Security Contact

2. **List of Operator's Subprocessors:**

[Box 29]

3.
Additional Data Security Measures:

[Box 30]

Document attached

Security Policy

Charmtech Labs LLC

Contents

POLICIES

Information Security Policy

Version	Date	Change/s	Author/s	Approver/s
1.0	08/15/14	Yury Puzis, Glenn Dausch	N/A	

Introduction

An Information Security Policy details the acceptable processes and practices for an organization to follow in order to protect the interests of Charmtech Labs LLC, as well as those of our customers, third-parties, employees, and other entities. This Information Security Policy is required reading for all users who are granted access to Charmtech Labs LLC's assets upon hire (before being granted access to the assets) and then annually. Charmtech Labs LLC's assets include anything owned or leased by Charmtech Labs LLC for operational and business use, to include (but not limited to) systems, data, computers, personal devices, applications, facilities, connections, individuals, documentation, and electronic media, whether located on Charmtech Labs LLC premise or off-site, and all Charmtech Labs LLC locations where cardholder data is present.

All users are required to follow this Information Security Policy at all times, unless a prior exception request has been reviewed and approved by a member of Charmtech Labs LLC Senior Management.

Scope

This policy applies to Charmtech Labs LLC employees, third-parties, service providers, contractors, temporary employees, and/or other staff members at Charmtech Labs LLC, whether conducting activities on Charmtech Labs LLC premises or off-site.

This policy applies to all systems, applications, and equipment owned or leased by Charmtech Labs LLC whether located on Charmtech Labs LLC premise or off-site, and all Charmtech Labs LLC locations where cardholder data is present.

Distribution

This policy is to be distributed to all users granted access to any Charmtech Labs LLC asset, to include Charmtech Labs LLC employees, third-parties, service providers, contractors, temporary employees, and/or other staff members.

The most current version of this policy is to be readily available and accessible from the internal file server.

Acknowledgement

This policy is to be reviewed and acknowledged via signature by all users granted access to any Charmtech Labs LLC asset, to include Charmtech Labs LLC employees, third-parties, service providers, contractors, temporary employees, and/or other staff members. Signature must be obtained from the user prior to their initial access and then annually as long as the access is maintained.

Exceptions

There are no exceptions to this policy. Requests for exceptions may be submitted to the Charmtech Labs LLC COO for review and approval using a “Policy Exception Request” form.

Violations

Individuals found to have violated this policy, whether intentionally or unintentionally, may be subject to disciplinary action and possible termination of employment.

Review Schedule

The next scheduled review date is January 2020 by COO Dr. Yury Puzis, to be approved by the CEO.

Why Information Security?

Information Security helps to:

- Safeguard Charmtech Labs LLC's assets and those belonging to our customers, third-parties, employees, and other entities.
- Support Charmtech Labs LLC's compliance with regulations, standards, and/or laws.
- Reduce risk to Charmtech Labs LLC's assets.
- Support the integrity of information and data.

Usage of Charmtech Labs LLC Assets

Charmtech Labs LLC's assets may only be used to support Charmtech Labs LLC business and operations. Users may not use Charmtech Labs LLC assets for personal use, unless authorized by their manager. Use of Charmtech Labs LLC assets must always be in a professional manner.

The following actions are never permitted when using Charmtech Labs LLC assets:

- Compromising confidentiality, integrity, and availability of Charmtech Labs LLC assets.
- Threatening, obscene, profane, offensive language or content.
- Harassing or violating others.
- Gaming, file sharing, music, and other activities.
- Work for another business, commercial venture, or non-Charmtech Labs LLC- sponsored activities.
- Advertising, purchasing, selling, and transacting non-Charmtech Labs LLC initiatives.
- Any illegal activities.

No Expectation of Privacy

Users are to expect that Charmtech Labs LLC may access or view their actions using Charmtech Labs LLC systems at any time and without prior notification. Charmtech Labs LLC reserves the right to disclose any user actions and communications to law enforcements or other parties without prior consent from the user.

Legal and Compliance Requirements

Charmtech Labs LLC is required to comply with several regulations, standards, and/or laws for our own organization, to meet our third-party contractual requirements, and also perhaps on behalf of our customers' compliance efforts.

See "Compliance List" for a full list of regulations and laws that Charmtech Labs LLC must comply with.

Roles and Responsibilities

Users are required to:

- Follow Charmtech Labs LLC policies at all times.
- Help Charmtech Labs LLC meet and maintain compliance with this Information Security Policy.
- Acknowledge their agreement with this Information Security Policy before their first access to Charmtech Labs LLC's assets and then annually for the lifetime of their access.
- Be aware of their role in supporting Charmtech Labs LLC's information security program.
- Comply with relevant regulations, standards, and/or laws governing Charmtech Labs LLC and Charmtech Labs LLC's customers, third-parties, and other applicable entities.
- Safeguard Charmtech Labs LLC's assets per the policies within this Information Security Policy.
- Report any deviation from this Information Security Policy to their direct manager immediately.

Managers are required to:

In addition to the above requirements:

- Ensure that their reports follow Charmtech Labs LLC policies at all times and understand their roles.
- Designate owners (if not themselves) for Charmtech Labs LLC assets under their control and management.
- Work with other groups to implement and maintain security controls for assets.
- Participate (as needed and directed) in incident response procedures.

Asset Owner/Managers are required to:

In addition to the above requirements:

- Manage the definition of user access to the assets under their control and management.
- Ensure that user access to their assets follows the principle of "least privileges".
- Verify that assets are protected sufficiently with the security controls.
- Properly assess and classify assets.
- Appoint a backup for when they are unavailable.

Data Security group is required to:

In addition to the above requirements:

- Oversee and manage compliance with Charmtech Labs LLC's policies.
- Perform risk assessments.
- Evaluate and select solutions to reduce risk to Charmtech Labs LLC assets.
- Write and distribute security policies to all users (as defined in the Introduction).
- Monitor and analyze security alerts and information and distribute to appropriate personnel.
- Define and deploy incident response and escalation procedures.
- Administer user accounts, including additions, deletions, and modifications.
- Monitor and control all access to data.
- Develop and implement Security Awareness and Training programs.
- Receive alerts from users and other systems 24/7/365.

- Provide direction to management on best security practices and recommended security controls and initiatives.

Senior Management is required to:

In addition to the above requirements:

- Champion best security practices from a “top down” approach.
- Take ultimate responsibility for safeguarding Charmtech Labs LLC’s assets.
- Accept residual risk resulting from assessment initiatives.

Individual Policies

1. Access Control

Without defined access privileges and control, users would be allowed to access systems and applications in Charmtech Labs LLC’s cardholder data environment, and be able to view, delete, and tamper with stored data, code, and configurations. Therefore, controlling who has access to what and what actions they are permitted to perform is important to support systems and applications transmitting, processing, and/or storing sensitive data from unauthorized access.

A careful review of each system and application should be performed based on results from risk assessment activities performed by Charmtech Labs LLC, and user’s granted access privileges based upon the principle of “business need-to-know” (where access is based on whether the individual requires access based upon their function or role). The general rule to follow is that all users start with no access privileges and are granted access to systems, applications, tools, etc. individually, as needed. All access granted is to be tracked in Security Priveleges document and reviewed on a quarterly basis as users may; leave the company, temporarily need access to specific systems, or, change positions where they no longer require access privileges.

Reference: Access Management Policy.

2. Anti-Virus

Viruses, and associated spyware, adware, and malware, can infiltrate Charmtech Labs LLC’s network, causing incalculable damage to systems and applications transmitting, processing, and/or storing sensitive data.

Viruses can shut down complete systems; spyware can capture user actions and take screenshots of cardholder data; and malware can spread through your network, causing damage to Charmtech Labs LLC, customers, and third-parties.

Anti-virus software must be deployed on all corporate servers, workstations, and gateways that are considered to be those commonly affected by viruses. This means that Unix-based systems may not require anti-virus to be deployed. Anti-virus software for Unix is available so Charmtech Labs LLC should determine whether it would be recommended to deploy such software for these systems based upon risk assessment results. The anti-virus software should be an up to date/current enough version that it protects against spyware and adware.

Reference: Anti-Virus Policy.

3. Critical Technologies

Critical technologies include remote access, wireless, removable media, laptops, tablets, personal data/digital assistants (PDAs), e-mail usage and Internet usage. These are all tools used to access Charmtech Labs LLC's network in a "non- standard" method, meaning they can be used remotely and not use a Charmtech Labs LLC workstation in a Charmtech Labs LLC location. Special care should be made when using these technologies as they are accessing Charmtech Labs LLC's network from an unknown location, therefore safeguarding the connection to the network is critical. It's also important to limit actions, which users can take, using these technologies to protect cardholder data wherever it is transmitted, processed, and/or stored.

Reference: Critical Technologies Policy.

4. Data Classifications

The purpose of classifying data is to be able to define and implement the appropriate level of security controls to protect it from unauthorized access and use. The higher the level of classification, the more intensive and comprehensive the security controls should be in place to protect it. Data can be in electronic or printed format, and may be transmitted, processed, and/or stored in the cardholder environment.

Printed and electronic data is to be classified in terms of its value to Charmtech Labs LLC, sensitivity, legal requirements, and impact if it is lost or falls into the 'wrong hands'. When performing a data classification exercise, it's critical to review the methods in which this data can be transmitted, stored, or used. Electronic data can be emailed, faxed, transmitted via instant message and/or other messaging technologies. Printed data can be faxed, hand delivered, scanned, and mailed. Data can be stored on systems, in code, workstations, devices, mobile media, and similar. Electronic data can be printed or copied to another workstation or system. Printed data can be retained in file cabinets and on desks.

"Confidential"

This type of classification is assigned to assets and data sets which, if lost, would cause serious harm to Charmtech Labs LLC, Charmtech Labs LLC's customers, Charmtech Labs LLC's third-parties, and others. Harmful effects can be from a financial, competitive, compliance, legal, branding, and/or reputation perspectives. Subsequently, it must be kept confidential.

Examples include cardholder data, financial plans, business and strategic plans, and customer lists.

"Restricted"

This type of classification is assigned to assets and data sets which, if lost, could potentially cause harm to Charmtech Labs LLC, Charmtech Labs LLC's customers, Charmtech Labs LLC's third-parties, and others; however it would not be unrepairable. Subsequently, it should be kept confidential as much as possible. By default, all Charmtech Labs LLC data is labeled as Restricted.

Examples include intranet content, performance evaluations, and internal communications (unless they contain confidential information).

“Unrestricted”

This type of classification is assigned to assets and data sets which are readily available and part of the public domain so would not cause any harm to Charmtech Labs LLC, Charmtech Labs LLC’s customers, Charmtech Labs LLC’s third-parties, and others. Subsequently, it does not require specific security controls.

Examples include Charmtech Labs LLC’s website, marketing materials, press releases, and external announcements.

Reference: Data Classification Policy.

5. Data Disposal

Assets and data sets need to be safeguarded from unauthorized access and use throughout the lifecycle. When no longer needed for business reasons, care should be taken to ensure that the asset and its data cannot be accessed or regenerated by an unauthorized user when disposed of or transferred to a new party. Data can be in electronic or printed format, and may be transmitted, processed, and/or stored in the cardholder environment.

Secure disposal methods are required for assets and data sets which are classified as “Confidential” or “Restricted”. Items classified as “Unrestricted” may be reused freely.

Disposal Requirements for Printed Data:

Labeled as “Confidential”

Printed documentation labeled as “Confidential” assets are required to be shredded using a cross-cut shredder. All areas handling documentation with sensitive information must have such a shredder located nearbyThese documents are to be securely retained up to their destruction. Users should be made aware of the importance of safely destructing these documents.

Assets Labeled as “Restricted”

“Restricted” assets are to be destroyed, and recorded, in the same manner as for those labeled as “Confidential”.

Assets Labeled as “Unrestricted”

“Unrestricted” assets are not required to be securely destroyed. If the data is not securely deleted, then checks must be made of each asset to ensure that there is no sensitive data retained prior to the asset being provided to another party.

Reference: Data Disposal Policy.

6. Data Handling

Assets and data sets need to be handled by users according to their classification in order to properly safeguard it from unauthorized access and usage (see Data Classification Policy). Data can be in electronic or printed format, and may be transmitted, processed, and/or stored in the cardholder environment. Charmtech Labs LLC's cardholder environment includes all systems, applications, equipment, individuals, locations, and connections used for, and involved with, the transmittal, processing, and/or storage of cardholder data.

Electronic data can be emailed, faxed, transmitted via instant message and other messaging technologies. Printed data can be faxed, hand delivered, scanned, and mailed. Data can be stored on systems, in code, workstations, devices, mobile media, and others. Electronic data can be printed or copied to another workstation or system. Printed data can be retained in file cabinets and on desks.

Handling Requirements for Assets and Data Sets Labeled as "Confidential":

Access	Business need-to-know only. Reviewed quarterly.
Non-Disclosure (NDA):	Charmtech Labs LLC third-parties and employees may only access these assets and data after signing an NDA. The system owner must then approve the distribution.
Changes:	Changes made to these assets and data sets must be approved by the Data Security group and the system owner prior to the change, recorded and retained for minimum of one year.
Email:	Only individuals approved by the Data Security group to transmit this data may do so, and then only if the email and its attachments are approved using a Charmtech Labs LLC-approved encryption method. A receipt request should be used or requested.
Internet:	This data may never be transmitted using a non-Charmtech Labs LLC email system or posted/communicated via the internet. This includes posting to websites or using internet email and messaging technologies.
Fax:	The person sending the fax with this data is required to be present at the fax machine to verify that it has been sent and is not stored in the memory. A receipt request should be used or requested.
Internal Mail:	This type of data should not be delivered over internal Charmtech Labs LLC mail, unless absolutely necessary and then a return receipt should be used or requested. It is preferable to deliver the item in-person.
External Mail:	This type of data is to be packaged in a secure manner and delivered by a commercial delivery service which can be tracked. A return receipt should be used or requested, such as a delivery signature.
Printing:	This type of data should not be printed unless absolutely needed for business purposes, and after approval from the Data Security group. The printing must be supervised.
Print Storage:	Printed data is required to be within eyesight or within possession at all times, or locked up in a secure manner or location.
Electronic Storage:	Stored data may not be retained in a readable format and is to be truncated, masked, or encrypted using a Charmtech Labs LLC-approved method. This includes data storage on workstations, systems, etc.

Handling Requirements for Assets and Data Sets Labeled as "Restricted":

Access	Business need-to-know only. Reviewed quarterly.
Non-Disclosure (NDA):	Charmtech Labs LLC third-parties and employees may only access these assets and data after signing a NDA.

Changes:	Changes made to these assets and data sets must follows the Charmtech Labs LLC Change Management Policy.
Email:	Only individuals approved by the Data Security group to transmit this data may do so, and then only if the email and its attachments are approved using a Charmtech Labs LLC-approved encryption method. A receipt request should be used or requested.
Internet:	This data may never be transmitted using a non-Charmtech Labs LLC email system or posted/communicated via the Internet. This includes posting to websites or using Internet email and messaging technologies.
Fax:	The person sending the fax with this data is required to be present at the fax machine to verify that it has been sent and is not stored in the memory. A receipt request should be used or requested.
Internal Mail:	This type of data should not be delivered over internal Charmtech Labs LLC mail, unless absolutely necessary and then a return receipt should be used or requested. It is preferable to deliver the item in-person.
External Mail:	This type of data is to be packaged in a secure manner and delivered by a commercial delivery service which can be tracked. A return receipt should be used or requested, such as a delivery signature.
Printing:	This type of data should not be printed unless absolutely needed for business purposes, and after approval from the Data Security group. The printing must be supervised.
Print Storage:	Printed data is required to be within eyesight or within possession at all times, or locked up in a secure manner or location.
Electronic Storage:	Stored data may not be retained in a readable format and is to be truncated, masked, or encrypted using a Charmtech Labs LLC-approved method. This includes data storage on workstations, systems, etc.

Handling Requirements for Assets and Data Sets Labeled as “Unrestricted”:

Access	Access is available to everyone
Non-Disclosure (NDA):	No NDA is required to distribute these assets or data
Changes:	Changes should follow the Change Management Policy
Email:	May be readily emailed
Internet:	May be readily transmitted; however caution should be used if posting to an external website to ensure that Charmtech Labs LLC’s reputation will not be harmed.
Fax:	May be readily faxed
Internal Mail:	May be delivered freely via internal mail
External Mail:	Mail be readily mailed outside of Charmtech Labs LLC
Printing:	May be readily printed
Print Storage:	Does not need to be stored securely
Electronic Storage:	Does not need to be stored securely

Reference: Data Handling Policy.

7. Data Retention

The retention period for assets and data sets may be affected by legal, industry, financial, and/or regulatory requirements. In order to reduce risk, however, assets and data sets should not be retained longer than absolutely required in the cardholder environment.

Each asset and data set (both electronic and printed formats) should be reviewed by a Legal point-of-contact to assess Charmtech Labs LLC's legal, industry, and regulatory requirements for its length of retention. The same exercise should be performed by the system owner as well as management to assess its industry requirements for retention. When completed, an analysis should be performed with the guiding principle that the item should be retained for the least amount of time as is possible.

Reference: Data Retention Policy.

8. Firewall Configuration and Management

Firewalls are critical to safeguard Charmtech Labs LLC's cardholder data environment as they filter access to systems and applications transmitting, processing, and/or storing this sensitive data.

Firewalls utilize established rule sets to allow or deny inbound or outbound network traffic between trusted and untrusted environments. Trusted environments include known zones that contain systems which transmit, process, and/or store cardholder data, and the internal network in general. Untrusted environments include Internet-facing access points, unknown environments, wireless networks, and zones which do not contain such systems which transmit, process, and/or store cardholder data. Firewalls are required to be placed at any Internet connection (to protect against traffic coming in from outside of Charmtech Labs LLC) and between internal network zones (should one zone contain sensitive systems and the other does not).

Reference: Firewall Configuration and Management Policy.

9. Incident Response

Security controls work together to reduce risk in Charmtech Labs LLC's environment. These controls may include intrusion detection systems, file integrity software, firewalls, logging, and many others. Many of these security controls are also used to notify the Data Security group whenever a suspected incident takes place or there is a system anomaly detected in Charmtech Labs LLC's cardholder environment. This allows the Data Security group to respond to and perform necessary activities to limit damage being caused. Charmtech Labs LLC users also play an important role in supporting the incident response process, by reporting anomalies they are encountering, such as a suddenly slower computer, accidental viewing of cardholder data in the clear, or a lost removable computer drive.

Reference: Incident Response Policy.

10. Log Management

Logging enables Charmtech Labs LLC to know who logged on to a system and when, and what actions did the user or application do. This is important to proactively monitor access to cardholder data and to identify anomalies, and also to review access should there be concern of an incident or breach to cardholder data being transmitted, processed, and/or stored.

Logging should be enabled on all systems where it is feasible to do so, which includes databases, servers, users desktops, applications (as applicable), networking equipment, wireless access points, etc.

11. Password Management

Passwords are the most common method of authenticating the identity of the user before allowing access to systems and applications in Charmtech Labs LLC's cardholder data environment. Subsequently, the effective management of user passwords is critical to support systems and applications transmitting, processing, and/or storing sensitive data from unauthorized access.

The user is responsible for constructing strong passwords and protecting the secrecy of their password. The Charmtech Labs LLC Data Security group is responsible for enforcing password parameters using automated access control methodologies, to include the required length of passwords, reuse, lockouts, history, change upon first login, secure storage, and other security controls. In addition, the Charmtech Labs LLC Data Security group is responsible for deploying additional authentication methods as defined by Charmtech Labs LLC Data Security group resulting from risk assessment activities (i.e.: two-factor authentication for remote access or for privileged access to critical systems and applications).

Users may not share their passwords with any other parties, even at their direct request. The user should notify the Data Security group should they receive a request for their password to initiate the incident response plan. In addition, users must take additional precautions to protect the security of their passwords by not writing it down, making it something which is readily known, or keeping it stored in an accessible location.

Users should not write down their passwords or store them electronically, unless using a pre-approved password storage system. In addition, users may not 'cache' or select an option to remember their password when online, as this may store the password insecurely. The Data Security group must store user passwords in a secure manner, protected from unauthorized access and in unreadable format.

12. Risk Assessment

The purpose and intent of Charmtech Labs LLC's security program is to reduce risk as much as possible to Charmtech Labs LLC's environment, while still enabling Charmtech Labs LLC to meet strategic and business objectives. Defining the risk level of assets (systems, equipment, applications, data, users, etc.) is critical in order to define the level of security controls required to safeguard those assets from harm. As it is impossible to reduce risk to zero, there will always be an amount of residual risk left. It is up to Charmtech Labs LLC Data Security Group to review and accept this level of risk. The higher the risk level associated with an asset, the more intensive and comprehensive the layers of security protecting the asset are required for cardholder data being transmitted, processed, and/or stored.

13. Router Configuration and Management

Routers are an integral part of Charmtech Labs LLC's network to safeguard Charmtech Labs LLC's cardholder data environment as they direct traffic to systems and applications transmitting, processing, and/or storing this sensitive data.

Routers route traffic will be based upon internal addresses and defined route tables to ensure that it arrives at its intended destination. Routers may also assist with functions performed by the firewall(s) where certain data packets are blocked. Subsequently, the protection of the router and of its configuration file is important in order to protect against external traffic being transmitted into trusted environments that contain systems which transmit, process, and/or store cardholder data, and the internal network in general.

Reference: Router Configuration and Management Policy.

14. Secure Configuration

As demands on time, productivity, and operations increase, the focus on securely configuring systems and network devices may suffer a lack of attention or a heightened amount of exceptions granted. Common security vulnerabilities, such as default passwords not being changed or a port remaining open after an exception request expires, can open up holes for an individual to gain unauthorized access to systems and applications transmitting, processing, and/or storing sensitive data.

Each system and networking component should be included in the annual risk assessment performed by Charmtech Labs LLC Data Security group, and their configurations compared against documented best security practices and standards. These documents should keep a record of the baseline configuration of the system and network component and deviations reviewed on a quarterly basis to ensure that risk cannot be introduced into the environment.

Reference: Secure Configuration Policy.

15. Security Awareness

Breaches can often be attributed to the actions performed by an organization’s employee(s), whether they are intentional or unintentional. If people are not provided with awareness of their roles and responsibilities when it comes to protecting Charmtech Labs LLC’s assets and data, they cannot be held responsible for their actions or know how their actions impact the security of Charmtech Labs LLC’s cardholder environment.

Users must receive security awareness training and sign an acknowledgment of their role in safeguarding Charmtech Labs LLC prior to being granted physical and logical access to Charmtech Labs LLC’s environment.

All users, for the entire length of time they are, or remain, connected to Charmtech Labs LLC’s environment, must receive security awareness training on an annual basis. This training may be provided to all users at one time, or may be staggered to take place on an annual basis from the user’s first day of employment or access granted. Training may occur in-person or via a computer-based training (CBT) format.

Attendance logs for those who attend security awareness training, both, provided upon hire and annually, must be kept by the Data Security group. Exceptions must be communicated to the user’s manager with a defined period of time that the user must take the training. Should the user not take the refresher training within that period, they are to be found in violation of this policy.

All users, for the entire length of time they are, or remain, connected to Charmtech Labs LLC’s environment, are to sign an agreement with Charmtech Labs LLC’s terms and conditions and acknowledgment of their role in safeguarding Charmtech Labs LLC’s environment on an annual basis. This should also occur when the security refresher training is provided.

Reference: Security Awareness Policy.

16. Testing and Scanning

Testing Charmtech Labs LLC’s systems and network is a critical component of protecting Charmtech Labs LLC’s cardholder environment from threats and vulnerabilities.

New vulnerabilities are discovered on a daily basis. Attackers can take advantage of these avenues to launch malicious attacks against Charmtech Labs LLC. Scans and penetration tests help find these problem areas proactively so they can be blocked.

Reference: Testing and Scanning Policy.

17. Third-Party Access and Management

Threats can be introduced to Charmtech Labs LLC’s environment simply by connecting a third-party without efficient security practices and controls in place. Should an attacker penetrate the third-party’s network, they may route their way via the connected third-party into Charmtech Labs LLC’s network. In some cases, third-parties have privileged access (meaning they have direct access to cardholder data in the production environment), thus gaining unauthorized access to the cardholder data environment.

Should an unauthorized user obtain access to Charmtech Labs LLC’s network via this route, they may do so under the pretense of being the third-party and therefore potentially penetrate systems, applications, and other networks unnoticed to gain additional access to sensitive data. This can lead to a security breach, causing harm to Charmtech Labs LLC’s finances, operations, and brand name.

A third-party, in Payment Card Industry (PCI) terms, may either transmit, process, and/or store cardholder data on behalf of Charmtech Labs LLC, but also may be connected to perform non PCI-related functions. Therefore, it is important to safeguard Charmtech Labs LLC from attackers masquerading as an authorized third-party, as well as proactively validating the security controls and practices in place at connected third-parties.

There are several types of third-parties, the most common being resellers, point of sale (POS) providers, Information Technology support companies, software application developers and vendors, shopping cart vendors, off-site storage vendors, data center and Web hosting providers, and Service Providers (those companies which transmit, process, and store cardholder data on Charmtech Labs LLC’s behalf..

Reference: Third-Party Access and Management Policy.

18. Time Synchronization

An accurate clock which synchronizes time across systems is critical to safeguard Charmtech Labs LLC’s cardholder data environment as identical timestamps support systems and applications transmitting, processing, and/or storing this sensitive data.

Identical system timestamps support the effectiveness and accuracy of several processes and technologies, to include services set to run at a specific time, log management and analysis, forensic investigations, server requests, commands, and more. It is common for system components to have their time begin to lag or change over an extended period of time. Subsequently, all system components need to maintain identical timestamps. A clock synchronization system needs to be implemented across all systems-in-scope, with a dedicated server or servers pulling the time from an established external time source. Those servers, in turn, distribute the time to the other systems.

User Signature

Users are to review this Information Security Policy and sign prior to gaining access to Charmtech Labs LLC's assets and network. Users are then to review and sign this Policy annually as well for the lifetime of their access.

___ New User ___ Annual Signature

User Name: ____

User Title: ____

User Company: ____

User Email: ____

User Phone Number: ____

User Signature: ____

Date: ____

Access Management Policy

Version	Date	Change/s	Author/s	Approver/s
1.0	08/15/14	Yury Puzis, Glenn Dausch	N/A	

Introduction

Without defined access privileges and control, users would be allowed to access systems and applications in Charmtech Labs LLC cardholder data environment, and be able to view, delete, and tamper with stored data, code, and configurations. Therefore, controlling who has access to what and what actions they are permitted to perform is important to support systems and applications transmitting, processing, and/or storing sensitive data from unauthorized access. Charmtech Labs LLC’s cardholder environment includes all systems, applications, equipment, individuals, locations, and connections used for, and involved with, the transmittal, processing, and/or storage of cardholder data.

A careful review of each system and application should be performed based on results from risk assessment activities performed by Charmtech Labs LLC Data Security group and user’s granted access privileges based upon the principle of “business need-to-know” (where access is based on whether the individual requires access based upon their function or role). The general rule to follow is that all users start with no access privileges and are granted access to systems, applications, tools, etc. individually, as needed. All access granted is to be tracked in ”Security Privileges” document, and reviewed on a quarterly basis as users may: leave the company, temporarily need access to specific systems, or, change positions where they no longer require access privileges.

Access to critical systems, applications, equipment, and data is required in order for the Charmtech Labs LLC to maintain business operations; however an user possessing privileges they do not require can lead to an intentional or unintentional security breach, causing harm to Charmtech Labs LLC’s finances, operations, and brand name.

Purpose

This Access Management Policy details the requirements for the granting, transferring, revoking and management of user access in Charmtech Labs LLC’s cardholder data environment for Payment Card Industry (PCI) compliance.

Scope

This policy applies to Charmtech Labs LLC employees, service providers, contractors, temporary employees, and/or other staff members at Charmtech Labs LLC, whether conducting activities on Charmtech Labs LLC premises or off-site.

This policy applies to all systems, applications, and equipment owned or leased by Charmtech Labs LLC whether located on Charmtech Labs LLC premise or off-site, and all Charmtech Labs LLC locations where cardholder data is present.

Distribution

This policy is to be distributed to all those with responsibilities for maintenance and management of networking equipment at Charmtech Labs LLC, to include Charmtech Labs LLC employees, service providers, contractors, temporary employees, and/or other staff members.

The most current version of this policy is to be readily available and accessible from the internal file server.

Exceptions

There are no exceptions to this policy. Requests for exceptions may be submitted to the Charmtech Labs LLC COO for review and approval using a “Policy Exception Request” form.

Violations

Individuals found to have violated this policy, whether intentionally or unintentionally, may be subject to disciplinary action and possible termination of employment.

Review Schedule

The next scheduled review date is January 2020 by COO Dr. Yury Puzis, to be approved by the CEO.

Policy

Access Privileges

Users are to be assigned access privileges based upon the individual’s business role and function, following the practice of business need-to-know and right-to-know. A structure of role based access control should be established so that specific functions receive standardized levels of access. Once assigned, the access granted should be reviewed to ensure that it is the lowest level necessary for the user to perform their job requirements.

Acknowledgement of Access

Users are to receive Charmtech Labs LLC’s information security policy and sign their acknowledgement of following Charmtech Labs LLC’s requirements prior to gaining access.

Tracking

All access granted, transferred, or revoked is to be tracked in ”Security Privileges” Document, and signed by the user’s manager and the system owner prior to being granted. This form should include the user’s name, location, department, date of access action taken, model after existing user (if applicable), and the access granted.

Review

Access privileges are to be reviewed on a quarterly basis by the user’s manager and the system owner.

Inactive or Disabled Accounts

Access accounts found to be inactive or not appropriately assigned are to be disabled/revoked and removed within 90 days.

Granting Access

Requests for access may be submitted to the Charmtech Labs LLC COO for review and approval using a ”Security Privilege Request” form and the user’s manager and the system owner are to approve the access prior to it being granted.

Changing Access

Requests for changing access may be submitted to the Charmtech Labs LLC COO for review and approval using a ”Security Privilege Request” or “Security Privilege Removal” forms and the user’s manager and the system owner are to approve the access prior to it being changed.

Removing Access

Requests for removing access may be submitted to the Charmtech Labs LLC COO for review and approval using a “Security Privilege Removal” form. If the user has been terminated from the company, the user’s manager must notify the COO to disable/revoke the user’s access by a specific date or immediately, should the termination be unfriendly. If the user holds privileged access to PCI systems or data, their access ID should be removed unless it is absolutely critical for business operations.

Privileged Users

Individuals with privileged IDs, such as security administrators, are to have separate accounts for their user-level activities and for their privileged functions. The user may not use their privileged ID for general user activities.

Anti-Virus Policy

Version	Date	Change/s	Author/s	Approver/s
1.0	08/15/14	Yury Puzis, Glenn Dausch	N/A	

Introduction

Viruses, and associated spyware, adware, and malware, can infiltrate Charmtech Labs LLC's network, causing incalculable damage to systems and applications transmitting, processing, and/or storing sensitive data. Charmtech Labs LLC's cardholder environment includes all systems, applications, equipment, individuals, locations, and connections used for, and involved with, the transmittal, processing, and/or storage of cardholder data.

Viruses can shut down complete systems; spyware can capture user actions and take screenshots of cardholder data; and malware can spread through your network, causing damage to Charmtech Labs LLC, and customers. Anti-virus software can help protect Charmtech Labs LLC systems from being affected by attacks and help safeguard Charmtech Labs LLC's finances, operations, and brand name.

Purpose

This Anti-Virus Policy details the requirements for the deployment, configuration, and management of anti-virus software in Charmtech Labs LLC's cardholder data environment for Payment Card Industry (PCI) compliance.

Scope

This policy applies to Charmtech Labs LLC employees, service providers, contractors, temporary employees, and/or other staff members at Charmtech Labs LLC, whether conducting activities on Charmtech Labs LLC premises or off-site.

This policy applies to all systems, applications, and equipment owned or leased by Charmtech Labs LLC whether located on Charmtech Labs LLC premise or off-site, and all Charmtech Labs LLC locations where cardholder data is present.

Distribution

This policy is to be distributed to all those with responsibilities for maintenance and management of networking equipment at Charmtech Labs LLC, to include Charmtech Labs LLC employees, service providers, contractors, temporary employees, and/or other staff members.

The most current version of this policy is to be readily available and accessible from the internal file server.

Exceptions

There are no exceptions to this policy. Requests for exceptions may be submitted to the Charmtech Labs LLC COO Dr. Yury Puzis for review and approval using a “Policy Exception Request” form.

Violations

Individuals found to have violated this policy, whether intentionally or unintentionally, may be subject to disciplinary action and possible termination of employment.

Review Schedule

The next scheduled review date is January 2020 by COO Dr. Yury Puzis, to be approved by the CEO Dr. Yevgen Borodin.

Policy

Deployment

Anti-virus software must be deployed on all corporate servers, workstations, and gateways which are considered to be those commonly affected by viruses. This means that Unix-based systems may not require anti-virus to be deployed. Anti-virus software for Unix is available so Charmtech Labs LLC should determine whether it would be recommended to deploy such software for these systems based upon risk assessment results. The anti-virus software should be an up to date/current enough version that it protects against spyware and adware.

Configuration

Configuration of the software must follow the vendor-provided guidance and standards, with exceptions reviewed and approved by the Data Security group. The software should be configured so that users cannot disable or tamper with it.

Scanning

Anti-virus software should be set to scan in “auto-protect” mode to automatically scan new files in creation, incoming and outgoing email attachments, and downloaded files. A full workstation scan should be set to be performed at a minimum, weekly, and a full server scan at a minimum, daily.

Lab Testing

If a scan is set to occur during lab testing, the anti-virus should take precedence and be run first. If the software needs to be disabled, it must be enabled again once the testing is complete.

Logging

Anti-virus event logs are to be generated and retained for at least 365 days. These logs should contain dates of scans performed and incidents found.

User Responsibilities

All users are to be aware/trained on how to prevent, detect, and respond to an incident which may be related to a virus, specifically users should know not to click on an attachment from an unknown person or if their system is running slow or acting up. Users are to report suspected incidents to the Data Security group.

Secure Configuration Policy

Version	Date	Change/s	Author/s	Approver/s
1.0	08/15/14	Yury Puzis, Glenn Dausch	N/A	

Introduction

As demands on time, productivity, and operations increase, the focus on securely configuring systems and network devices may suffer a lack of attention or a heightened amount of exceptions granted. Common security vulnerabilities, such as default passwords not being changed or a port remaining open after an exception request expires, can open up holes for an individual to gain unauthorized access to systems and applications transmitting, processing, and/or storing sensitive data. Charmtech Labs LLC's cardholder environment includes all systems, applications, equipment, individuals, locations, and connections used for, and involved with, the transmittal, processing, and/or storage of cardholder data.

Each system and networking component should be included in the annual risk assessment performed by Charmtech Labs LLC Data Security group, and their configurations compared against documented best security practices and standards. These documents should keep a record of the baseline configuration of the system and network component and deviations reviewed on a quarterly basis to ensure that risk cannot be introduced into the environment.

Deviations from secure configurations can lead to an intentional or unintentional security breach, causing harm to Charmtech Labs LLC's finances, operations, and brand name.

Purpose

This Secure Configuration Policy details the requirements for the safe configuration of systems and networking equipment in Charmtech Labs LLC's cardholder data environment for Payment Card Industry (PCI) compliance.

Scope

This policy applies to Charmtech Labs LLC employees, third-parties, service providers, contractors, temporary employees, and/or other staff members at Charmtech Labs LLC, whether conducting activities on Charmtech Labs LLC premises or off-site.

This policy applies to all systems, applications, and equipment owned and/or leased by Charmtech Labs LLC whether located on Charmtech Labs LLC premises or off-site, and all Charmtech Labs LLC locations where cardholder data is present.

Distribution

This policy is to be distributed to all those with responsibilities for maintenance and management of networking equipment at Charmtech Labs LLC, to include Charmtech Labs LLC employees, third-parties, service providers, contractors, temporary employees, and/or other staff members.
The most current version of this policy is to be readily available and accessible from the internal file server.

Exceptions

There are no exceptions to this policy. Requests for exceptions may be submitted to the Charmtech Labs LLC COO Dr. Yury Puzis for review and approval using a “Policy Exception Request” form.

Violations

Individuals found to have violated this policy, whether intentionally or unintentionally, may be subject to disciplinary action and possible termination of employment.

Review Schedule

The next scheduled review date is January 2020 by COO Dr. Yury Puzis, to be approved by the CEO Dr. Yevgen Borodin.

Policy

Documentation

Secure configuration standards are to be documented for each system and networking component in the cardholder environment. These documents are to be based on accepted best security configuration practices (to include those from SANS, CIS, ISO) or vendor guidelines (Microsoft, Apache, Oracle) or a combination of both. Should the guidance not be applicable in Charmtech Labs LLC's environment or it has been decided to be excluded from Charmtech Labs LLC's secure configuration standards, an exception is required to be created and approved by Charmtech Labs LLC COO. Charmtech Labs LLC secure configuration standards must be updated whenever there is a change made to the environment, a change made to the system or networking component, or an exception is made.

Basic Requirements

The following are required:

- Services and applications, if not in use, are to be disabled.
- All insecure services, applications, and protocols must be reviewed and assessed for their risk. Charmtech Labs LLC COO must review and sign their acceptance of the risk. An exception request, to include their business justification, must be retained for the lifetime of the exception.
- All firewall ports should be restricted to only those required for the environment. Requests to open up a port or make changes must follow Charmtech Labs LLC's firewall policies.
- Default vendor passwords must be changed prior to deployment into production, and then Charmtech Labs LLC password policies maintained on the server.
- Patches must be kept current on the servers, and follow Charmtech Labs LLC's patch management policies.
- Change control must follow Charmtech Labs LLC's change management policies.
- Access permissions must be restricted to business-need only and follow the principle of least privilege.
- Root admin should not be used unless absolutely necessary.
- Access by applications and users must follow Charmtech Labs LLC's logging policies.
- Remote access must be two-factor authentication and over secure channels.

Data Classification Policy

Version	Date	Change/s	Author/s	Approver/s
1.0	08/15/14	Yury Puzis, Glenn Dausch	N/A	

Introduction

The purpose of classifying data is to be able to define and implement the appropriate level of security controls to protect it from unauthorized access and use. The higher the level of classification, the more intensive and comprehensive the security controls should be in place to protect it. Data can be in electronic or printed format, and may be transmitted, processed, and/or stored in the cardholder environment. Charmtech Labs LLC's cardholder environment includes all systems, applications, equipment, individuals, locations, and connections used for, and involved with, the transmittal, processing, and/or storage of cardholder data.

Printed and electronic data is to be classified in terms of its value to Charmtech Labs LLC, sensitivity, legal requirements, and impact if it is lost or falls into the 'wrong hands'. When performing a data classification exercise, it's critical to review the methods in which this data can be transmitted, stored, or used. Electronic data can be emailed, faxed, transmitted via instant message and/or other messaging technologies. Printed data can be faxed, hand delivered, scanned, and mailed. Data can be stored on systems, in code, workstations, devices, mobile media, and similar. Electronic data can be printed or copied to another workstation or system. Printed data can be retained in file cabinets and on desks.

Classifying data can help protect Charmtech Labs LLC data from unauthorized access and usage, and help safeguard Charmtech Labs LLC's finances, operations, and brand name.

Purpose

This Data Classification Policy details the requirements for the classification of assets and data in Charmtech Labs LLC's cardholder data environment for Payment Card Industry (PCI) compliance.

Scope

This policy applies to Charmtech Labs LLC employees, third-parties, service providers, contractors, temporary employees, and/or other staff members at Charmtech Labs LLC, whether conducting activities on Charmtech Labs LLC premises or off-site.

This policy applies to all systems, applications, and equipment owned or leased by Charmtech Labs LLC whether located on Charmtech Labs LLC premise or off-site, and all Charmtech Labs LLC locations where cardholder data is present.

Distribution

This policy is to be distributed to all those with responsibilities for maintenance and management of networking equipment at Charmtech Labs LLC, to include Charmtech Labs LLC employees, third-parties, service providers, contractors, temporary employees, and/or other staff members.

The most current version of this policy is to be readily available and accessible from the internal file server.

Exceptions

There are no exceptions to this policy. Requests for exceptions may be submitted to the Charmtech Labs LLC COO Dr. Yury Puzis for review and approval using a "Policy Exception Request" form.

Violations

Individuals found to have violated this policy, whether intentionally or unintentionally, may be subject to disciplinary action and possible termination of employment.

Review Schedule

The next scheduled review date is January 2020 by COO Dr. Yury Puzis, to be approved by the CEO Dr. Yevgen Borodin.

Policy

Asset and Data Identification

Any asset (system, workstation, removable media, mobile media, etc.) and data being processed, transmitted, and/or stored in the cardholder environment is to be identified and documented, along with the asset owner's name, location, and contact information.

Asset and Data Evaluation

A risk assessment exercise should be performed to determine level of risk associated with each asset and data set. The list should be documented and assigned a classification of High, Medium, or Low in terms of its value to Charmtech Labs LLC, sensitivity, legal requirements, and impact if lost or misused. Once this is completed, the evaluation should be reviewed and approved by Data Security group.

Classification Terminology

Should the asset or data set receive one or more *High* results during the evaluation exercise, it should be labeled as "Confidential". If there are no *High* results and the asset or data set carries one or more *Medium* results, it should be labeled as "Restricted". If the asset or data set receives no *High* or *Medium* results, it may be labeled as "Unrestricted".

Security Controls

The level of security controls to be in place to safeguard the asset or data set from unauthorized access and misuse will increase with its classification level. For example, a database storing encrypted cardholder data should still be classified as *High* and therefore "Confidential", even though the contents are encrypted, as the loss of this data may still cause non-compliance with legal requirements and harm Charmtech Labs LLC's reputation. This database would require the highest level of security controls to be in place, to include, but not limited to, being placed behind a firewall and an intrusion detection/prevention system, have restricted access permissions, maintain file integrity software, and have active logging enabled. An asset or data set classified as "Unrestricted" may be freely released externally and communicated, and may be readily accessible to both internal and external users.

Data Handling

Once the asset or data set have been classified, it is to be transmitted, processed, used, and/or stored following the methods outlined in the Data Handling Policy. An asset or data set without an assigned classification is to be treated as "Confidential" until it is properly classified.

Incident Response

Should a "Confidential" asset or data set be intentionally or unintentionally accessed, viewed, or used by an unauthorized party, the incident response plan is to be initiated. Should it be "Restricted" asset or data set, the Data Security group should evaluate the repercussions of the event and initiate the incident response plan as appropriate.

Classification Details

“Confidential”

This type of classification is assigned to assets and data sets which, if lost, would cause serious harm to Charmtech Labs LLC, Charmtech Labs LLC’s customers, Charmtech Labs LLC’s third-parties, and others. Harmful effects can be from a financial, competitive, compliance, legal, branding, and/or reputation perspectives. Subsequently, it must be kept confidential.

Examples include cardholder data, financial plans, business and strategic plans, and customer lists.

“Restricted”

This type of classification is assigned to assets and data sets which, if lost, could potentially cause harm to Charmtech Labs LLC, Charmtech Labs LLC’s customers, Charmtech Labs LLC’s third-parties, and others; however it would not be unrepairable. Subsequently, it should be kept confidential as much as possible. By default, all Charmtech Labs LLC data is labeled as Restricted.

Examples include intranet content, performance evaluations, and internal communications (unless they contain confidential information).

“Unrestricted”

This type of classification is assigned to assets and data sets which are readily available and part of the public domain so would not cause any harm to Charmtech Labs LLC, Charmtech Labs LLC’s customers, Charmtech Labs LLC’s third-parties, and others. Subsequently, it does not require specific security controls.

Examples include Charmtech Labs LLC’s website, marketing materials, press releases, and external announcements.

Requests for Access to “Confidential” or “Restricted” Assets or Data

The system owner is ultimately responsible for individuals and applications which have access to their assets, and are to review all access requests. The system owner is to review the access permissions on a quarterly basis in tandem with the quarterly access control review exercise.

Awareness

Users are to be trained and made aware of the classifications and their handling requirements. Users who have business requirements to view, access, and use “Confidential” and “Restricted” assets and data are to receive specialized training on how to properly handle those items.

Data Handling Policy

Version	Date	Change/s	Author/s	Approver/s
1.0	08/15/14	Yury Puzis, Glenn Dausch	N/A	

Introduction

Assets and data sets need to be handled by users according to their classification in order to properly safeguard it from unauthorized access and usage (see Data Classification Policy). Data can be in electronic or printed format, and may be transmitted, processed, and/or stored in the cardholder environment. Charmtech Labs LLC's cardholder environment includes all systems, applications, equipment, individuals, locations, and connections used for, and involved with, the transmittal, processing, and/or storage of cardholder data.

Electronic data can be emailed, faxed, transmitted via instant message and other messaging technologies. Printed data can be faxed, hand delivered, scanned, and mailed. Data can be stored on systems, in code, workstations, devices, mobile media, and others. Electronic data can be printed or copied to another workstation or system. Printed data can be retained in file cabinets and on desks.

Handling assets and data according to its classification level can help protect Charmtech Labs LLC data from unauthorized access and usage, and help safeguard Charmtech Labs LLC's finances, operations, and brand name.

Purpose

This Data Handling Policy details the requirements for the transmission, storing, and usage of assets and data in Charmtech Labs LLC's cardholder data environment for Payment Card Industry (PCI) compliance.

Scope

This policy applies to Charmtech Labs LLC employees, third-parties, service providers, contractors, temporary employees, and/or other staff members at Charmtech Labs LLC, whether conducting activities on Charmtech Labs LLC premises or off-site.

This policy applies to all systems, applications, and equipment owned or leased by Charmtech Labs LLC whether located on Charmtech Labs LLC premise or off-site, and all Charmtech Labs LLC locations where cardholder data is present.

Distribution

This policy is to be distributed to all those with responsibilities for maintenance and management of networking equipment at Charmtech Labs LLC, to include Charmtech Labs LLC employees, third-parties, service providers, contractors, temporary employees, and/or other staff members.

The most current version of this policy is to be readily available and accessible from the internal file server.

Exceptions

There are no exceptions to this policy. Requests for exceptions may be submitted to the Charmtech Labs LLC COO Dr. Yury Puzis for review and approval using a “Policy Exception Request” form.

Violations

Individuals found to have violated this policy, whether intentionally or unintentionally, may be subject to disciplinary action and possible termination of employment.

Review Schedule

The next scheduled review date is January 2020 by COO Dr. Yury Puzis, to be approved by the CEO Dr. Yevgen Borodin.

Policy

Cardholder Data

Cardholder data may never be transmitted using any end-user methodologies unless specifically approved by the Data Security group with a valid business need. If required to transmit cardholder data, it must be in unreadable format (for example, encrypted, masked, truncated). Users may also not store cardholder data without specific approval to do so from the Data Security group at which point it must also be retained in a protected format. The only exception is for users who need to view cardholder numbers for business reasons, these users must be approved by Data Security group and may only view the number individually (meaning one by one).

Handling Requirements for Assets and Data Sets Labeled as “Confidential”:

Access	Business need-to-know only. Reviewed quarterly.
Non-Disclosure (NDA):	Charmtech Labs LLC third-parties and employees may only access these assets and data after signing an NDA. The system owner must then approve the distribution.
Changes:	Changes made to these assets and data sets must be approved by the Data Security group and the system owner prior to the change, recorded and retained for minimum of one year.
Email:	Only individuals approved by the Data Security group to transmit this data may do so, and then only if the email and its attachments are approved using a Charmtech Labs LLC-approved encryption method. A receipt request should be used or requested.
Internet:	This data may never be transmitted using a non-Charmtech Labs LLC email system or posted/communicated via the internet. This includes posting to websites or using internet email and messaging technologies.
Fax:	The person sending the fax with this data is required to be present at the fax machine to verify that it has been sent and is not stored in the memory. A receipt request should be used or requested.
Internal Mail:	This type of data should not be delivered over internal Charmtech Labs LLC mail, unless absolutely necessary and then a return receipt should be used or requested. It is preferable to deliver the item in-person.
External Mail:	This type of data is to be packaged in a secure manner and delivered by a commercial delivery service which can be tracked. A return receipt should be used or requested, such as a delivery signature.
Printing:	This type of data should not be printed unless absolutely needed for business purposes, and after approval from the Data Security group. The printing must be supervised.
Print Storage:	Printed data is required to be within eyesight or within possession at all times, or locked up in a secure manner or location.
Electronic Storage:	Stored data may not be retained in a readable format and is to be truncated, masked, or encrypted using a Charmtech Labs LLC-approved method. This includes data storage on workstations, systems, etc.

Handling Requirements for Assets and Data Sets Labeled as “Restricted”:

Access	Business need-to-know only. Reviewed quarterly.
Non-Disclosure	Charmtech Labs LLC third-parties and employees may only access these assets and

(NDA):	data after signing a NDA.
Changes:	Changes made to these assets and data sets must follows the Charmtech Labs LLC Change Management Policy.
Email:	Only individuals approved by the Data Security group to transmit this data may do so, and then only if the email and its attachments are approved using a Charmtech Labs LLC-approved encryption method. A receipt request should be used or requested.
Internet:	This data may never be transmitted using a non-Charmtech Labs LLC email system or posted/communicated via the Internet. This includes posting to websites or using Internet email and messaging technologies.
Fax:	The person sending the fax with this data is required to be present at the fax machine to verify that it has been sent and is not stored in the memory. A receipt request should be used or requested.
Internal Mail:	This type of data should not be delivered over internal Charmtech Labs LLC mail, unless absolutely necessary and then a return receipt should be used or requested. It is preferable to deliver the item in-person.
External Mail:	This type of data is to be packaged in a secure manner and delivered by a commercial delivery service which can be tracked. A return receipt should be used or requested, such as a delivery signature.
Printing:	This type of data should not be printed unless absolutely needed for business purposes, and after approval from the Data Security group. The printing must be supervised.
Print Storage:	Printed data is required to be within eyesight or within possession at all times, or locked up in a secure manner or location.
Electronic Storage:	Stored data may not be retained in a readable format and is to be truncated, masked, or encrypted using a Charmtech Labs LLC-approved method. This includes data storage on workstations, systems, etc.

Handling Requirements for Assets and Data Sets Labeled as "Unrestricted":

Access	Access is available to everyone
Non-Disclosure (NDA):	No NDA is required to distribute these assets or data
Changes:	Changes should follow the Change Management Policy
Email:	May be readily emailed
Internet:	May be readily transmitted; however caution should be used if posting to an external website to ensure that Charmtech Labs LLC's reputation will not be harmed.
Fax:	May be readily faxed
Internal Mail:	May be delivered freely via internal mail
External Mail:	Mail be readily mailed outside of Charmtech Labs LLC
Printing:	May be readily printed
Print Storage:	Does not need to be stored securely
Electronic Storage:	Does not need to be stored securely

Data Retention Policy

Version	Date	Change/s	Author/s	Approver/s
1.0	08/15/14	Yury Puzis, Glenn Dausch	N/A	

Introduction

The retention period for assets and data sets may be affected by legal, industry, financial, and/or regulatory requirements. In order to reduce risk, however, assets and data sets should not be retained longer than absolutely required in the cardholder environment. Charmtech Labs LLC's cardholder environment includes all systems, applications, equipment, individuals, locations, and connections used for, and involved with, the transmittal, processing, and/or storage phase(s) of cardholder data.

Each asset and data set (both electronic and printed formats) should be reviewed by a Legal point-of-contact to assess Charmtech Labs LLC's legal, industry, and regulatory requirements for its length of retention. The same exercise should be performed by the system owner as well as management to assess its industry requirements for retention. When completed, an analysis should be performed with the guiding principle that the item should be retained for the least amount of time as is possible.

The retention of assets and data for the minimum length of time possible under law and to support business operations can help protect Charmtech Labs LLC data from unauthorized access and usage, and help safeguard Charmtech Labs LLC's finances, operations, and brand name.

Purpose

This Data Retention Policy details the requirements for the retention of assets and data in Charmtech Labs LLC's cardholder data environment for Payment Card Industry (PCI) compliance.

Scope

This policy applies to Charmtech Labs LLC employees, third-parties, service providers, contractors, temporary employees, and/or other staff members at Charmtech Labs LLC, whether conducting activities on Charmtech Labs LLC premises or off-site.

This policy applies to all systems, applications, and equipment owned or leased by Charmtech Labs LLC whether located on Charmtech Labs LLC premise or off-site, and all Charmtech Labs LLC locations where cardholder data is present.

Distribution

This policy is to be distributed to all those with responsibilities for maintenance and management of networking equipment at Charmtech Labs LLC, to include Charmtech Labs LLC employees, third-parties, service providers, contractors, temporary employees, and/or other staff members.

The most current version of this policy is to be readily available and accessible from the internal file server.

Exceptions

There are no exceptions to this policy. Requests for exceptions may be submitted to the Charmtech Labs LLC COO for review and approval using a “Policy Exception Request” form.

Violations

Individuals found to have violated this policy, whether intentionally or unintentionally, may be subject to disciplinary action and possible termination of employment.

Review Schedule

The next scheduled review date is January 2020 by COO Dr. Yury Puzis, to be approved by the CEO.

Policy

Retention of Cardholder Data

Cardholder data will not be retained on Charmtech Labs LLC servers.

Retention of Sensitive Authentication Data

Sensitive Authentication Data (the magnetic strip, PIN blocks, CVV) may never be stored after authorization.

Responsibilities

The system owner or the data owner is ultimately responsible for ensuring cardholder data are not retained.

Third-Parties

Third-parties will have no access to cardholder data environment.

Data Disposal Policy

Version	Date	Change/s	Author/s	Approver/s
1.0	08/15/14	Yury Puzis, Glenn Dausch	N/A	

Introduction

Assets and data sets need to be safeguarded from unauthorized access and use throughout the lifecycle. When no longer needed for business reasons, care should be taken to ensure that the asset and its data cannot be accessed or regenerated by an unauthorized user when disposed of or transferred to a new party. Data can be in electronic or printed format, and may be transmitted, processed, and/or stored in the cardholder environment. Charmtech Labs LLC's cardholder environment includes all systems, applications, equipment, individuals, locations, and connections used for, and involved with, the transmittal, processing, and/or storage of cardholder data.

Secure disposal and deletion methods are required for assets and data sets which are classified as "Confidential" or "Restricted". Items classified as "Unrestricted" may be reused freely.

The secure disposal and deletion of assets and data according to its classification level can help protect Charmtech Labs LLC data from unauthorized access and use, and continue to safeguard Charmtech Labs LLC's finances, operations, and brand name.

Purpose

This Data Disposal Policy details the requirements for the disposal of assets and deletion of data in Charmtech Labs LLC's cardholder data environment for Payment Card Industry (PCI) compliance.

Scope

This policy applies to Charmtech Labs LLC employees, third-parties, service providers, contractors, temporary employees, and/or other staff members at Charmtech Labs LLC, whether conducting activities on Charmtech Labs LLC premises or off-site.

This policy applies to all systems, applications, and equipment owned or leased by Charmtech Labs LLC whether located on Charmtech Labs LLC premise or off-site, and all Charmtech Labs LLC locations where cardholder data is present.

Distribution

This policy is to be distributed to all those with responsibilities for maintenance and management of networking equipment at Charmtech Labs LLC, to include Charmtech Labs LLC employees, third-parties, service providers, contractors, temporary employees, and/or other staff members.

The most current version of this policy is to be readily available and accessible from the internal file server.

Exceptions

There are no exceptions to this policy. Requests for exceptions may be submitted to the Charmtech Labs LLC COO Dr. Yury Puzis for review and approval using a “Policy Exception Request” form.

Violations

Individuals found to have violated this policy, whether intentionally or unintentionally, may be subject to disciplinary action and possible termination of employment.

Review Schedule

The next scheduled review date is January 2020 by COO Dr. Yury Puzis, to be approved by the CEO Dr. Yevgen Borodin.

Policy

Disposal Requirements for Printed Data:

Labeled as “Confidential” or “Restricted”

Printed documentation labeled as “Confidential” assets are required to be shredded using a cross-cut shredder. All areas handling documentation with sensitive information must have such a shredder located nearby. These documents are to be securely retained up to their destruction. Users should be made aware of the importance of safely destructing these documents.

Assets Labeled as “Unrestricted”

“Unrestricted” assets are not required to be securely destroyed. If the data is not securely deleted, then checks must be made of each asset to ensure that there is no sensitive data retained prior to the asset being provided to another party.

Responsibilities

The system owner or the data owner is ultimately responsible for ensuring that electronic and printed media is disposed of in a secure manner, and the users’ managers are responsible for ensuring that their employees follow these policies. The Data Security group is responsible for performing the actual destruction or deletion of data.

Critical Technologies Policy

Version	Date	Change/s	Author/s	Approver/s
1.0	08/15/14	Yury Puzis, Glenn Dausch	N/A	

Introduction

Critical technologies include remote access, wireless, removable media, laptops, tablets, personal data/digital assistants (PDAs), e-mail usage and Internet usage. These are all tools used to access Charmtech Labs LLC’s network in a “non- standard” method, meaning they can be used remotely and not use a Charmtech Labs LLC workstation in a Charmtech Labs LLC location. Special care should be made when using these technologies as they are accessing Charmtech Labs LLC’s network from an unknown location, therefore safeguarding the connection to the network is critical. It’s also important to limit actions, which users can take, using these technologies to protect cardholder data wherever it is transmitted, processed, and/or stored. Charmtech Labs LLC’s cardholder environment includes all systems, applications, equipment, individuals, locations, and connections used for, and involved with, the transmittal, processing, and/or storage of cardholder data.

Properly safeguarding these technologies is critical to help protect Charmtech Labs LLC from unauthorized users causing harm to Charmtech Labs LLC’s finances, operations, and brand name.

Purpose

This Critical Technologies Policy details the requirements for the usage of remote access, modems, laptops, tablets, and PDAs in Charmtech Labs LLC's cardholder data environment for Payment Card Industry (PCI) compliance. The other listed critical technologies are detailed in other Charmtech Labs LLC Policies.

Scope

This policy applies to Charmtech Labs LLC employees, third-parties, service providers, contractors, temporary employees, and/or other staff members at Charmtech Labs LLC, whether conducting activities on Charmtech Labs LLC premises or off-site.

This policy applies to all systems, applications, and equipment owned and/or leased by Charmtech Labs LLC whether located on Charmtech Labs LLC premises or off-site, and all Charmtech Labs LLC locations where cardholder data is present.

Distribution

This policy is to be distributed to all those with responsibilities for maintenance and management of networking equipment at Charmtech Labs LLC, to include Charmtech Labs LLC employees, third-parties, service providers, contractors, temporary employees, and/or other staff members.

The most current version of this policy is to be readily available and accessible from the internal file server.

Exceptions

There are no exceptions to this policy. Requests for exceptions may be submitted to the Charmtech Labs LLC COO Dr. Yury Puzis for review and approval using a "Policy Exception Request" form.

Violations

Individuals found to have violated this policy, whether intentionally or unintentionally, may be subject to disciplinary action and possible termination of employment.

Review Schedule

The next scheduled review date is January 2020 by COO Dr. Yury Puzis, to be approved by the CEO Dr. Yevgen Borodin.

Policy

Remote Access

Remote access into cardhoder data environment must always be comprised of two-factor authentication. This means that there is required to be authentication with something the user knows (password, passphrase) and something the user has (key fob, fingerprint, or individual certificate). These are to be used in conjunction with the user's individual user ID. Remote access must be via console SSH and logged. Remote access may not be used unless for business purposes, and all users must be approved by the Charmtech Labs LLC CEO prior to being granted this access. Only Charmtech Labs LLC-approved remote access technologies may be used. The session will automatically disconnect after 30 minutes and the user will be required to re-authenticate. Third-parties must only be granted remote access permissions and capability after being assessed for risk and approved by the CEO, monitored while in use, and then immediately disconnected after use. All users may not copy, move, or store cardholder data using this technology.

Modems

The use of modems is not authorized.

Laptops, Tablets, and PDAs

All users are to be approved by their manager prior to being granted the equipment and access to the environment. Charmtech Labs LLC's access control and password management policies are to apply to the usage of this equipment, and users must be required to authenticate with a unique user ID and password. Charmtech Labs LLC's devices may only be utilized for Charmtech Labs LLC business purposes and must be Charmtech Labs LLC sanctioned. Users may not use their own devices unless previously authorized to do so by the CEO.

Firewall Configuration and Management Policy

Version	Date	Change/s	Author/s	Approver/s
1.0	08/15/14	Yury Puzis, Glenn Dausch	N/A	

Introduction

Firewalls are critical to safeguard Charmtech Labs LLC’s cardholder data environment as they filter access to systems and applications transmitting, processing, and/or storing this sensitive data. Charmtech Labs LLC’s cardholder environment includes all systems, applications, equipment, individuals, locations, and connections used for, and involved with, the transmittal, processing, and/or storage of cardholder data.

Firewalls utilize established rule sets to allow or deny inbound or outbound network traffic between trusted and untrusted environments. Trusted environments include known zones that contain systems which transmit, process, and/or store cardholder data, and the internal network in general. Untrusted environments include Internet-facing access points, unknown environments, wireless networks, and zones which do not contain such systems which transmit, process, and/or store cardholder data. Firewalls are required to be placed at any Internet connection (to protect against traffic coming in from outside Charmtech Labs LLC) and between internal network zones (should one zone contain sensitive systems and the other does not).

Should an unauthorized user obtain access to Charmtech Labs LLC’s network via a route unprotected with a firewall, they may then potentially penetrate systems, applications, and other networks to gain additional access to sensitive data. This can lead to a security breach, causing harm to Charmtech Labs LLC’s finances, operations, and brand name.

Purpose

This Firewall Configuration and Management Policy details the requirements for the configuration, placement, and maintenance of firewalls in Charmtech Labs LLC’s cardholder data environment for Payment Card Industry (PCI) compliance.

Scope

This policy applies to Charmtech Labs LLC employees, third-parties, service providers, contractors, temporary employees, and other staff members at Charmtech Labs LLC, whether conducting activities on Charmtech Labs LLC premises or off-site.

This policy applies to all systems, applications, and equipment owned or leased by Charmtech Labs LLC whether located on Charmtech Labs LLC premises or off-site, and all Charmtech Labs LLC locations where cardholder data is present.

Distribution

This policy is to be distributed to all those with responsibilities for maintenance and management of networking equipment at Charmtech Labs LLC, to include Charmtech Labs LLC employees, third-parties, service providers, contractors, and temporary employees.

The most current version of this policy is to be readily available and accessible from the internal file server.

Exceptions

There are no exceptions to this policy. Requests for exceptions may be submitted to the Charmtech Labs LLC COO Dr. Yury Puzis for review and approval using a “Policy Exception Request” form.

Violations

Individuals found to have violated this policy, whether intentionally or non-intentionally, may be subject to disciplinary action and possible termination of employment.

Review Schedule

The next scheduled review date is January 2020 by COO Dr. Yury Puzis, to be approved by the CEO Dr. Yevgen Borodin.

Policy

Placement

Trusted environments include known zones that contain systems which transmit, process, and/or store cardholder data, and the internal network in general. Untrusted environments include Internet-facing access points, unknown environments, wireless networks, and zones which do not contain such systems which transmit, process, and/or store cardholder data.

Firewalls are required to be placed at any Internet connection (to protect against traffic coming in from outside Charmtech Labs LLC) and between internal network zones (should one zone contain sensitive systems and the other does not). There may not be direct inbound or outbound access without the placement of a firewall between trusted and untrusted environments.

Environments which are not segmented from the cardholder data environment with firewalls or other form of segmentation (such as a VLAN) must be considered a “flat network” and part of the cardholder environment. All systems, users, equipment etc. within this other environment will be in-scope for PCI assessments.

Network Diagram

A network diagram (“Network Diagram” document) is to be maintained which accurately depicts the networking equipment, systems, applications, wireless networks, and other applicable components of the cardholder data environment. This includes all inbound and outbound connections, all connected third-parties, locations, security controls in place (i.e.: Intrusion Detection/Prevention Systems), and network segregation in place.

This network diagram must be reviewed and updated after changes are made to the environment, or annually, whichever comes first. The review is to be performed by the Data Security group and the date of last review documented on the diagram.

Access Rules

Firewalls are to have implicit deny-all rules, unless specific traffic is authorized. Internal outbound traffic from systems within the cardholder environment may only access predefined IP addresses, and admit all inbound and outbound traffic on the Charmtech Labs LLC network environment to only what is required for business purposes.

Firewall rule sets (“Firewall Rule Sets” document) are to be documented and kept current, and Firewall reviewed by COO on a semi-annual basis, at a minimum. The COO must document the review and results in a “Firewall Review” log. The COO is to review and sign-off on the findings. Exceptions are to be submitted following the Exception process noted earlier in this Policy.

Change Management

Changes may only be made to the configuration of the firewall and the firewall rule sets after a review of the impact of the change has been performed by the COO. This is to help protect against the possibility of inadvertently introducing open avenues for attack. Once the review has been performed, the change documentation and description of any residual risk from performing the change is to be reviewed and accepted by the COO

Firewall changes are to be tested in a tested environment prior to being placed into the production environment. Care should be made to carefully monitor deployments of the change once introduced into the production environment when more permissive rules have been introduced.

Traffic Control

Stateful inspection firewalls are to be used, with Network Address Translation (NAT) in place to prevent against IP Masquerading (the broadcast of IP addresses from the internal network to the Internet).

Ports and Services

Only those ports and services which are required for business purposes may be enabled. The firewalls are to explicitly deny inbound and outbound traffic using any other ports and services.

A list of approved ports and services and their business justifications is to be kept current by COO and is to be updated after any changed is made (“Approved Ports, Services and Protocols” document). Changes are to follow the change management process described earlier in this document.

Protocols

Only those protocols which are required for business purposes may be enabled. The firewalls are to explicitly deny inbound and outbound traffic using any other protocols.

Protocols which are considered “risky” may lead to granting an avenue of attack. Types of “risky” protocols include Telnet, rlogin, and FTP. As any protocol could be considered “risky” if configured incorrectly, care should be made to safeguard against this occurring. These protocols should also not be permitted for use on personal computers with access to the cardholder data environment.

A list of approved protocols and their business justifications is to be kept current by COO and is to be updated after any changed is made. (“Approved Ports, Services and Protocols” document). Changes are to follow the change management process described earlier in this document.

Access Controls

Access to the firewall should be limited to only those individuals with a business need-to-know. Individual authentication, meaning a unique userID and unique password, is to be used by the administrators, unless an Admin account has been specifically approved by COO.

Remote access to the firewalls may only be performed using a secure network protocol, such as SSH, and users must use two-factor authentication (the user must possess something they have and something they know in addition to their userID).

Password management is to follow the password requirements specified in the Password Management Policy.

Event Management and Response

Firewall logs are to be generated, reviewed, and maintained for a period of 1 year to provide an audit trail. Logs should include capture of events which have an impact on the configuration of the firewall, unsuccessful attempts to establish a connection via the firewall, packets which are directed to terminate at the firewall.

Incidents, whether suspected or actual, are to be responded to in accordance with the Incident Response Plan.

Scanning

Firewalls are to be included in the vulnerability scanning initiatives performed by Charmtech Labs LLC and Control Scan.

Time Synchronization

Network Time Protocol (NTP) or other time synchronization tool is to be used for the firewalls and synced with the other systems in the cardholder environment to maintain consistent times.

Personal Firewalls

Any computers with access to the Internet which are able to access Charmtech Labs LLC's network are to have a personal firewall enabled and active. This includes computers used by any parties included in the scope of this policy. The personal firewall should be deployed in such a way that it cannot be tampered with and altered by unauthorized individuals.

Logical Management of Network Components

The following individuals are responsible for the logical management of networking equipment:

Configuration and maintenance of firewall rule sets	Ivan Fesenko	System Administrator
Installation of firewalls	Ivan Fesenko	System Administrator
Deployment of firewalls	Ivan Fesenko	System Administrator
Network diagram maintenance	Ivan Fesenko	System Administrator
Reviews of firewall rule set change requests	Ivan Fesenko	System Administrator
Approvals of firewall rule set change requests	Ivan Fesenko	System Administrator

Router Configuration and Management Policy

Version	Date	Change/s	Author/s	Approver/s
1.0	08/15/14	Yury Puzis, Glenn Dausch	N/A	

Introduction

Routers are an integral part of Charmtech Labs LLC's network to safeguard Charmtech Labs LLC's cardholder data environment as they direct traffic to systems and applications transmitting, processing, and/or storing this sensitive data. Charmtech Labs LLC's cardholder environment includes all systems, applications, equipment, individuals, locations, and connections used for, and involved with, the transmittal, processing, and/or storage of cardholder data.

Routers route traffic will be based upon internal addresses and defined route tables to ensure that it arrives at its intended destination. Routers may also assist with functions performed by the firewall(s) where certain data packets are blocked. Subsequently, the protection of the router and of its configuration file is important in order to protect against external traffic being transmitted into trusted environments that contain systems which transmit, process, and/or store cardholder data, and the internal network in general.

Should an unauthorized user obtain access to Charmtech Labs LLC's network they may potentially penetrate systems, applications, and other networks to gain additional access to sensitive data. This can lead to a security breach, causing harm to Charmtech Labs LLC's finances, operations, and brand name.

Purpose

This Router Configuration and Management Policy details the requirements for the configuration, placement, and maintenance of routers in Charmtech Labs LLC's cardholder data environment for Payment Card Industry (PCI) compliance.

Scope

This policy applies to Charmtech Labs LLC employees, third-parties, service providers, contractors, temporary employees, and/or other staff members at Charmtech Labs LLC, whether conducting activities on Charmtech Labs LLC premises or off-site.

This policy applies to all systems, applications, and equipment owned or leased by Charmtech Labs LLC whether located on Charmtech Labs LLC premise or off-site, and all Charmtech Labs LLC locations where cardholder data is present.

Distribution

This policy is to be distributed to all those with responsibilities for maintenance and management of networking equipment at Charmtech Labs LLC, to include Charmtech Labs LLC employees, third-parties, service providers, contractors, temporary employees, and/or other staff members.

The most current version of this policy is to be readily available and accessible from the internal file server.

Exceptions

There are no exceptions to this policy. Requests for exceptions may be submitted to the Charmtech Labs LLC COO Dr. Yury Puzis for review and approval using a “Policy Exception Request” form.

Violations

Individuals found to have violated this policy, whether intentionally or unintentionally, may be subject to disciplinary action and possible termination of employment.

Review Schedule

The next scheduled review date is January 2020 by COO Dr. Yury Puzis, to be approved by the CEO Dr. Yevgen Borodin.

Policy

Placement

Trusted environments include known zones that contain systems which transmit, process, and/or store cardholder data, and the internal network in general. Untrusted environments include internet-facing access points, unknown environments, wireless networks, and zones which do not contain such systems that transmit, process, and/or store cardholder data.

Configuration Services

Routers are to have configuration services defined to support the operating system (OS), as the OS translates the established access control list (ACL) to the router. Configurations are to be configured to permit only authorized inbound and outbound traffic to the trusted environments for only matters required for business purposes.

Router files are to be documented and kept current, and reviewed by the COO on a semi-annual basis, at a minimum. The COO must document the review and results in a Router Review log. The COO is to review and sign-off on the findings. Exceptions are to be submitted following the *Exceptions* process noted earlier in this Policy.

Change Management

Changes may only be made to the configuration of the router and its configuration files after review of the impact of the change has been performed by the COO. This is to help protect against the possibility of inadvertently introducing open avenues for attack. Once the review has been performed, the change documentation and description of any residual risk from performing said change is to be reviewed and accepted by the COO.

Router changes are to be tested in a test environment prior to being placed into the production environment. Care should be taken to carefully monitor deployments of the change once introduced into the production environment when more permissive rules have been introduced.

Synchronization of Router Files

Router files are required to be synchronized upon start-up. Changes that are made only to the running configuration won't be retained upon reboot; therefore, changes must be made to the configuration copy in the RAM or to the start-up configuration.

Access Controls

Access to the routers should be limited to only those individuals with a business need-to-know. Individual authentication (a unique userID and unique password) is to be used by the administrators, unless an Admin account has been specifically approved by COO.

Remote access to the routers may only be performed using a secure network protocol, such as SSH, and users must use two-factor authentication (the user must possess something they have and something they know in addition to their userID).

Password management is to follow the password requirements specified in the Password Management Policy.

Event Management and Response

Router logs will not be generated since we are using a virtual router from Amazon Web Services which does not have this functionality.

Incidents, whether suspected or actual, are to be responded to in accordance with the Incident Response Plan.

Time Synchronization

Usage of virtual routers on Amazon Web Services precludes router time synchronization. The servers are synchronizing on their own.

Logical Management of Network Components

The following individuals are responsible for the logical management of networking equipment:

Configuration and maintenance of router files	Ivan Fesenko	System Administrator
Installation of routers	Ivan Fesenko	System Administrator
Deployment of routers	Ivan Fesenko	System Administrator
Network diagram maintenance	Ivan Fesenko	System Administrator
Reviews of router config file change requests	Ivan Fesenko	System Administrator
Approvals of router config file change requests	Ivan Fesenko	System Administrator

Security Awareness Policy

Version	Date	Change/s	Author/s	Approver/s
1.0	08/15/14	Yury Puzis, Glenn Dausch	N/A	

Introduction

Breaches can often be attributed to the actions performed by an organization's employee(s), whether they are intentional or unintentional. If people are not provided with awareness of their roles and responsibilities when it comes to protecting Charmtech Labs LLC's assets and data, they cannot be held responsible for their actions or know how their actions impact the security of Charmtech Labs LLC's cardholder environment. The cardholder environment includes systems, applications, equipment, individuals, locations, and connections used for, and involved with, the transmittal, processing, and/or storage of cardholder data.

All persons with physical and logical access to Charmtech Labs LLC's environment, whether employees, third-parties, service providers, contractors, temporary employees, and/or other staff members, must be trained on their role in protecting Charmtech Labs LLC from threats to help safeguard Charmtech Labs LLC's finances, operations, and brand name.

Purpose

This Security Awareness Policy details the requirements for the security awareness and training of users with physical and logical access to Charmtech Labs LLC's cardholder data environment for Payment Card Industry (PCI) compliance.

Scope

This policy applies to Charmtech Labs LLC employees, third-parties, service providers, contractors, temporary employees, and/or other staff members at Charmtech Labs LLC, whether conducting activities on Charmtech Labs LLC premises or off-site.

This policy applies to all systems, applications, and equipment owned or leased by Charmtech Labs LLC whether located on Charmtech Labs LLC premise or off-site, and all Charmtech Labs LLC locations where cardholder data is present.

Distribution

This policy is to be distributed to all those with responsibilities for maintenance and management of networking equipment at Charmtech Labs LLC, to include Charmtech Labs LLC employees, third-parties, service providers, contractors, temporary employees, and/or other staff members.

The most current version of this policy is to be readily available and accessible from the internal file server.

Exceptions

There are no exceptions to this policy. Requests for exceptions may be submitted to the Charmtech Labs LLC COO for review and approval using a “Policy Exception Request” form.

Violations

Individuals found to have violated this policy, whether intentionally or unintentionally, may be subject to disciplinary action and possible termination of employment.

Review Schedule

The next scheduled review date is January 2020 by COO Dr. Yury Puzis, to be approved by the CEO.

Policy

Connection of Users

Users must receive security awareness training and sign an acknowledgment of their role in safeguarding Charmtech Labs LLC prior to being granted physical and logical access to Charmtech Labs LLC's environment.

Refresher Training

All users, for the entire length of time they are, or remain, connected to Charmtech Labs LLC's environment, must receive security awareness training on an annual basis. This training may be provided to all users at one time, or may be staggered to take place on an annual basis from the user's first day of employment or access granted. Training may occur in-person or via a computer-based training (CBT) format.

Logs

Attendance logs ("Attendance of Security Awarness Training" document) for those who attend security awareness training, both, provided upon hire and annually, must be kept by the Data Security group. Exceptions must be communicated to the user's manager with a defined period of time that the user must take the training. Should the user not take the refresher training within that period, they are to be found in violation of this policy.

Acknowledgements

All users, for the entire length of time they are, or remain, connected to Charmtech Labs LLC's environment, are to sign an agreement with Charmtech Labs LLC's terms and conditions and acknowledgment of their role in safeguarding Charmtech Labs LLC's environment on an annual basis. This should also occur when the security refresher training is provided.

Security Awareness Vehicles

Supporting vehicles for promoting security awareness are to be maintained throughout the year. These can include newsletter articles, posters, email reminders, and messages acknowledged upon user login.

Technical Training

In addition to the above, those who have admin or privileged access or roles with systems which transmit, process, and store cardholder data must receive additional technical training to further reinforce and supplement their knowledge of security practices.

Testing and Scanning Policy

Version	Date	Change/s	Author/s	Approver/s
1.0	08/15/14	Yury Puzis, Glenn Dausch	N/A	

Introduction

Testing Charmtech Labs LLC’s systems and network is a critical component of protecting Charmtech Labs LLC’s cardholder environment from threats and vulnerabilities. Charmtech Labs LLC’s cardholder environment includes all systems, applications, equipment, individuals, locations, and connections used for, and involved with, the transmittal, processing, and/or storage of cardholder data.

New vulnerabilities are discovered on a daily basis. Attackers can take advantage of these avenues to launch malicious attacks against Charmtech Labs LLC. Scans and penetration tests help find these problem areas proactively so they can be blocked. The difference between scans and penetration tests is that scans are performed using automated tools of Charmtech Labs LLC’s Internet Protocol (IP) addresses and report on vulnerabilities, rating them by level of criticality. Penetration tests are performed by trained individuals who are granted explicit permission by Charmtech Labs LLC to actively try to penetrate systems and applications as if they are an attacker.

Unauthorized access can potentially lead to a security breach, causing harm to Charmtech Labs LLC’s finances, operations, and brand name.

Purpose

This Testing and Scanning Policy details the requirements for the testing of, and reporting on, vulnerabilities in Charmtech Labs LLC’s cardholder data environment for Payment Card Industry (PCI) compliance.

Scope

This policy applies to Charmtech Labs LLC employees, third-parties, service providers, contractors, temporary employees, and other staff members at Charmtech Labs LLC, whether conducting activities on Charmtech Labs LLC premises or off-site.

This policy applies to all systems, applications, and equipment owned and/or leased by Charmtech Labs LLC whether located on Charmtech Labs LLC premises or off-site, and all Charmtech Labs LLC locations where cardholder data is present.

Distribution

This policy is to be distributed to all those with responsibilities for maintenance and management of networking equipment at Charmtech Labs LLC, to include Charmtech Labs LLC employees, third-parties, service providers, contractors, and temporary employees.

The most current version of this policy is to be readily available and accessible from the internal file server.

Exceptions

There are no exceptions to this policy. Requests for exceptions may be submitted to the Charmtech Labs LLC COO Dr. Yury Puzis for review and approval using a “Policy Exception Request” form.

Violations

Individuals found to have violated this policy, whether intentionally or unintentionally, may be subject to disciplinary action and possible termination of employment.

Review Schedule

The next scheduled review date is January 2020 by COO Dr. Yury Puzis, to be approved by the CEO Dr. Yevgen Borodin.

Policy

Authorization

Prior authorization in writing must be obtained from the COO before any type of testing is performed of Charmtech Labs LLC's network and systems. The individual performing the testing must be vetted first to possess the qualifications, experience, and skills to perform such testing. The tools and software used must also be approved by the COO. No Charmtech Labs LLC users may ever perform their own testing of any kind on Charmtech Labs LLC's network, systems, and assets. This is in direct violation with Charmtech Labs LLC policies.

Scoping

All systems defied as in-scope for the cardholder environment are to be tested and scanned per this policy. All external network connections are to be included in the scope.

Remediation

Findings for any of the types of testing methods below are to be ranked as Critical, High, Medium, or Low, as it relates to the risk assessment results performed for the systems, applications, and data sets in the cardholder environment. This meaning that the risk assessment results correlate with the scan rating results and increase upon sensitivity. Scan findings rated as Critical and High must be remediated within 1 day, while findings rated as Medium and Low are to be closed within 7 days. Once the findings have been closed, a rescan or retest must be performed to verify that they were closed adequately. Charmtech Labs LLC COO must review these results and provide sign-off.

Retention

All scan and test results, whether initial or remediated findings, must be retained for the purposes of compliance with PCI DSS for a minimum of 5 years. These reports and materials are to be classified as "Confidential" due to the sensitive nature of the content, and handled per the Data Handling and Retention Policies.

External Vulnerability Scans

External scans are required to be performed on a quarterly basis by a PCI authorized third-party scanning vendor (ASV) to meet PCI compliance, however additional external scans performed outside these windows may be performed by a qualified, experienced, and skilled Charmtech Labs LLC employee. The third-party must review and sign a Non-Disclosure Agreement (NDA) and receive a copy of Charmtech Labs LLC's information security policies. External scans must be performed on a quarterly basis, at a minimum, and/or after any significant change to the network environment.

Testing of Third Parties

All third-parties connecting to Charmtech Labs LLC's network must show evidence that they have performed the scans and tests listed above and have closed any Critical and High vulnerabilities. This evidence is to be provided prior to permitting the third-party access to Charmtech Labs LLC's network and systems.

Third-Party Access and Management Policy

Version	Date	Change/s	Author/s	Approver/s
1.0	08/15/14	Yury Puzis, Glenn Dausch	N/A	

Introduction

Threats can be introduced to Charmtech Labs LLC's environment simply by connecting a third-party without efficient security practices and controls in place. Should an attacker penetrate the third-party's network, they may route their way via the connected third-party into Charmtech Labs LLC's network. In some cases, third-parties have privileged access (meaning they have direct access to cardholder data in the production environment), thus gaining unauthorized access to the cardholder data environment. Charmtech Labs LLC's cardholder environment includes all systems, applications, equipment, individuals, locations, and connections used for, and involved with, the transmittal, processing, and/or storage of cardholder data.

Should an unauthorized user obtain access to Charmtech Labs LLC's network via this route, they may do so under the pretence of being the third-party and therefore potentially penetrate systems, applications, and other networks unnoticed to gain additional access to sensitive data. This can lead to a security breach, causing harm to Charmtech Labs LLC's finances, operations, and brand name.

A third-party, in Payment Card Industry (PCI) terms, may either transmit, process, and/or store cardholder data on behalf of Charmtech Labs LLC, but also may be connected to perform non PCI-related functions. Therefore, it is important to safeguard Charmtech Labs LLC from attackers masquerading as an authorized third-party, as well as proactively validating the security controls and practices in place at connected third-parties.

There are several types of third-parties, the most common being resellers, point of sale (POS) providers, Information Technology support companies, software application developers and vendors, shopping cart vendors, off-site storage vendors, data center and Web hosting providers, and Service Providers (those companies which transmit, process, and store cardholder data on Charmtech Labs LLC's behalf.

Purpose

This Third-Party Access and Management Policy details the requirements for the evaluation, connection, compliance, and management of third-parties to Charmtech Labs LLC's cardholder data environment.

Scope

This policy applies to Charmtech Labs LLC employees, third-parties, service providers, contractors, temporary employees, and other staff members at Charmtech Labs LLC, whether conducting activities on Charmtech Labs LLC premises or off-site.

This policy applies to all systems, applications, and equipment owned or leased by Charmtech Labs LLC whether located on Charmtech Labs LLC premises or off-site, and all Charmtech Labs LLC locations where cardholder data is present.

Distribution

This policy is to be distributed to all those with responsibilities for maintenance and management of security controls and practices at Charmtech Labs LLC, to include Charmtech Labs LLC employees, third-parties, service providers, contractors, and temporary employees.

The most current version of this policy is to be readily available and accessible from the internal file server.

Exceptions

There are no exceptions to this policy. Requests for exceptions may be submitted to the Charmtech Labs LLC COO Dr. Yury Puzis for review and approval using a “Policy Exception Request” form.

Violations

Individuals found to have violated this policy, whether intentionally or non-intentionally, may be subject to disciplinary action and possible termination of employment.

Review Schedule

The next scheduled review date is January 2020 by COO Dr. Yury Puzis, to be approved by the CEO Dr. Yevgen Borodin.

Policy

Assessment of Risk

Third-parties must be given a risk assessment prior to being connected to the Charmtech Labs LLC cardholder data environment. No third-party may be connected to the Charmtech Labs LLC environment prior to receiving this assessment. Should a third-party have not received this risk assessment and is currently connected, the risk assessment is to be performed before they may be reconnected. This assessment is to include discovery of threats which may lead to potential vulnerabilities.

Once the review has been performed, the third-party is to close gaps found, and the remaining findings and description of risk are to be reviewed and accepted by the CEO.

Network Diagram

A network diagram is to be maintained which accurately depicts all connected third-parties, along with networking equipment, systems, applications, wireless networks, and other applicable components of the cardholder data environment.

List of Third-Parties

Charmtech Labs LLC is to maintain a current list of connected third-parties with details of whether they have direct access to the cardholder environment. This is to clearly denote which third-parties have privileged access and so special attention may be paid to them during session monitoring. The list of third-parties is to also include their PCI compliance status and date of, whether they have accepted by their acquiring bank or VISA or have performed a SAQ (whichever is applicable to their Level as defined above).

PCI Compliance Status

The status of connected third-parties achieving PCI compliance is to be reviewed annually. All third-parties with direct access to the cardholder environment must obtain PCI compliance or have an official exception provided by their acquiring bank or VISA. Should a third-party with privileged access not have obtained this compliance status, they are to document in writing their efforts in doing so with the target completion date. Charmtech Labs LLC is to monitor the compliance efforts of these third-parties.

Terms and Conditions

All connected third-parties are to sign a Non-Disclosure Agreement (NDA). Contracts with Service Providers are to contain terms and conditions, as well as an agreement to safeguard Charmtech Labs LLC's cardholder data in all its formats from generation to its destruction, and signed by the third-party prior to connection to Charmtech Labs LLC's network. No third-party may be connected to the Charmtech Labs LLC environment prior to signing their agreement with Charmtech Labs LLC's terms and conditions. Should a third-party have not signed their agreement and is currently connected, they are required to do so before they may be reconnected.

Terms and conditions should contain the following, but not limited to, the third-party's obligation to:

- Protect Charmtech Labs LLC’s cardholder data and environment.
- Follow Charmtech Labs LLC’s policies and procedures at all times, unless there is specific approval from the CEO.
- Use only Charmtech Labs LLC-approved security controls and practices.
- Communicate any suspected compromise of third-party systems connected to Charmtech Labs LLC’s network.
- Escalate suspected breaches and incidents to the Charmtech Labs LLC within 3 hours.
- Retain and dispose of electronic and paper cardholder data media in a secure manner.
- Comply with federal and industry laws and regulations.
- Train individuals with access to Charmtech Labs LLC systems and data on effective safeguard measures.
- Maintain security awareness amongst personnel.
- Conduct criminal background checks on all individuals with access to Charmtech Labs LLC’s network, systems, and data. Background checks are to be performed prior to granting individuals access.
- Removing access permissions immediately upon termination of the individual.
- Maintaining appropriate access control methods, including two-factor remote access.
- Only attempting to connect to Charmtech Labs LLC’s network during authorized periods, and disconnecting when the work is completed.
- Permitting Charmtech Labs LLC to perform periodic reviews, and forensic investigations upon Charmtech Labs LLC CEO determination.
- Physically and logically segregating Charmtech Labs LLC systems, networks, and data from those belonging to any other clients.
- Implementing logging and audit trail requirements.
- Notifying and obtaining agreement from Charmtech Labs LLC prior to outsourcing work to other third-parties.

Change Management

Any changes made by the third-party in regards to their security controls and practices as well as organizational process changes must be communicated to Charmtech Labs LLC. Charmtech Labs LLC is to review the change as to its potential impact on Charmtech Labs LLC. This is to help protect against the possibility of inadvertently introducing open avenues for attack. Once the review has been performed, the change documentation and description of any residual risk from the third-party performing the change is to be reviewed and accepted by the CEO.

Any system or application changes with impact on Charmtech Labs LLC are to be tested by the third-party in a test environment prior to being placed into the production environment.

Event Management and Response

Logs for Charmtech Labs LLC systems, applications, and equipment managed by the third-parties are to be generated, reviewed, and maintained in accordance with the Log Management Policy to provide an audit trail. Logs are to be synced to a safeguarded central location.

Incidents, whether suspected or actual, are to be reported to Charmtech Labs LLC within 3 hours so they may be responded to in accordance with the Incident Response Plan. Determination of the third-party’s role in incident response and containment should be clearly defined.

Security Awareness

Training is to be provided by the third-party at an appropriate level by function. Individuals with access to Charmtech Labs LLC's cardholder environment are to be provided with more detailed training upon hire and then on an annual basis, with a focus on the protection of Charmtech Labs LLC's cardholder environment and technical training. Other company individuals are to receive general security awareness training upon hire and then annually.

Access Controls

Access to the Charmtech Labs LLC's cardholder environment is to be limited to only those individuals with a business need-to-know. Individual authentication, meaning a unique userID and unique password, is to be used.

Remote access may only be performed using a secure network protocol, such as SSH, and users must use two-factor authentication (the user must possess something they have and something they know in addition to their userID).

Password management is to follow the password requirements specified in the Password Management Policy.

Monitoring and Managing Third-Party Access

Third-party access may only be permitted with prior authorization from the COO, and is to be connected immediately after use. COO are to monitor the access at all times. In some cases, access is granted to third-parties on a 24/7/365 basis. These types of access should be approved by the CEO prior to access being granted, and COO is to periodically monitor the connection without prior notification to the third-party.

The third-party may not attempt to access Charmtech Labs LLC's network without prior authorization at anytime, and doing so may result in the initiation of the incident response plan.

Testing and Scanning

The third-party is to agree to periodic security controls and practices review by Charmtech Labs LLC, and to be included in the vulnerability scanning initiatives performed by Charmtech Labs LLC. Additional testing procedures, such as penetration testing and application assessments, may also be performed as needed.

In the instance of a breach to Charmtech labs LLC's cardholder environment, Charmtech Labs LLC reserves the right to perform forensic activities on the third-party's environment.

Segregation

The third-party is to logically and physically separate Charmtech Labs LLC's systems, network, and data from any other clients (if applicable). There may not be any shared environments without the explicit permission of Charmtech Labs LLC.

Incident Response Policy

Version	Date	Change/s	Author/s	Approver/s
1	08/15/14	Yury Puzis, Glenn Dausch	N/A	

The person who discovers the incident will immidiately notify the First Response Team by email. First Response Team includes the system administrator and the COO of Charmtech Labs LLC.The system administrator will immidiately take measures to rectify and terminate the incident (if possible) until the First Response Team analyzes the problem and resolves it in a fundamental way.

The COO will coordinate with the sytem administrator to make sure a log of the incident is created, in a form of a ticket in Jira, specifically mentioning (when available):

1) The name of the reporter
2) Time of the report
3) The nature of the incident
4) Equipment or persons involved
5) Name of system being targeted, along with operating system, IP address, and location.
6) How the incident was detected
7) When the event was first noticed that supported the idea that the incident occurred
8) Is the equipment affected business critical?
9) Severity of the potential impact
10) IP address and any information about the origin of the attack.

The COO, the system administrator, and the person(s) responsible for the affected module will discuss the incident over the phone or Skype and determine response strategy, adding to the ticket relevant information as follows:

1) Is the incident real or perceived?
2) Is the incident still in progress?
3) What data or property is threatened and how critical is it?
4) What is the impact on the business should the attack succeed? Minimal, serious, or critical?
5) What system or systems are targeted, where are they located physically and on the network?
6) Is the incident inside the trusted network?
7) Will the response alert the attacker and do we care?
8) What type of incident is this? Example: virus, worm, intrusion, abuse, damage.

The team members will then take actions to properly and fundamentally rectify the incident and restore the systems. After the incident was handled the COO will update the ticket with:

1) Information about how the incident was rectified, and the effectiveness of the response
2) Recommended changes to prevent similar incidents in the future (creating new tickets if necessary)
3) Incident evidence: copies of logs, email, and other communication, names of people involved.

The COO will also:

1) Notify proper external agencies (e.g., the police) if prosecution of the intruder is possible.
2) Assess the damage to the organization and estimate both the damage cost and the cost of the containment efforts