RIDER

This is a Rider to the contract (including any terms of services or terms of use or any other policies, terms, agreements, or understandings referenced therein) between the Commack Union Free School District ("the District") and Prentke Romich Company d/b/a PRC-Saltillo ("the Contractor"), that is being entered into for a Three year term for the use of NuVoice PASS and ChatEditor pursuant to the attached quote ("the Contract") (collectively, the Contract and Rider are referred to as "the Agreement").

To the extent that the provisions of this Rider and the annexed Data Privacy Agreement are inconsistent with any terms set forth in the Contract, the provisions of this Rider and the annexed Data Privacy Agreement will control.

1. Plan for Security and Protection of Personally Identifiable Information

   A. "District Data" means all information obtained by the Contractor from the District or by the Contractor in connection with the Services provided by the Contractor pursuant to this Agreement, including but not limited to business, administrative and financial data, intellectual property, student and personnel data, and metadata. The term, "District Data" does not include any information made publicly available by the District, except PII from student and personnel data which will be considered "District Data" regardless of whether or not it is made public.

   B. "Personally Identifiable Information" or "PII" includes, but is not limited to: (i) a person's name or address or the names or addresses of a student's parents or other family members; (ii) any personal identifier (e.g., SSN, student number or biometric record); (iii) indirect identifiers (e.g., date of birth, place of birth, or mother's maiden name); (iv) other information that alone or in combination is linked or linkable to a specific individual and would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances to identify the individual with reasonable certainty; and (v) any information requested by a person who the District or Contractor reasonably believes knows the identity of the person to whom a record relates.

   C. The Contractor represents and warrants that it will comply with all District policies and State, federal and local laws, regulations, rules and requirements related to the confidentiality, security and privacy of District Data.

   D. The Contractor represents and warrants that District Data received by the Contractor will be used only to perform Contractor's obligations pursuant to the Agreement and for no other purpose.

E. The Contractor represents and warrants that it will only collect data from the District or District employees or other End Users (the term "End Users" means the individuals authorized by the District to access and use services provided by the Contractor pursuant to the Agreement) that is necessary to fulfill the Contractor's duties pursuant to the Agreement.

F. The Parties agree that all rights including all intellectual property rights in and to District Data will remain the exclusive property of the District and that the Contractor has a limited, non-exclusive license to use District Data solely to perform the Services pursuant to the Agreement.

G. If the Contractor has access to District Data that is subject to the Family Educational Rights and Privacy Act ("FERPA"), the Contractor acknowledges that for purposes of the Agreement it will be designated as a "school official" with a "legitimate educational interest" pursuant to FERPA and its implementing regulations, and the Contractor agrees to abide by the limitations and requirements imposed on school officials.

H. The Contractor must execute and deliver the Data Privacy Agreement annexed hereto as Exhibit A simultaneously with the execution and delivery of this Rider. The terms of the Data Privacy Agreement are hereby incorporated into this Rider.

I. All the provisions of this Paragraph will survive the expiration or sooner termination of the Agreement.

2. Indemnification by the District: If the Contract has any provision that requires the District to indemnify, defend and/or hold harmless the Contractor, such provision will be void and have no force or effect.

3. Entire Agreement/No End User Agreements: The Agreement contains the entire agreement of the parties with respect to the subject matter thereof and supersedes any and all other agreements, understandings and representations, written or oral, by and between the parties. In the event that any part of the Agreement references terms of service or terms of use or any other policies, terms, agreements or understandings, the applicable policies, terms, agreements or understandings are those that were in effect on the date of the Contract, unless the applicable policies, terms, agreements or understandings were modified pursuant to Paragraph 6 of this Rider. In the event that the Consultant requires District employees or other End Users to enter into terms of use agreements or other agreements or understandings, whether electronic, click-through, verbal or in writing, those agreements and/or understandings will be null, void and without effect, and the terms of the Agreement will apply.

4. Termination: The Agreement may be terminated by the District immediately upon the Contractor's breach of the Contractor's obligations set forth in paragraph 1 of this Rider. Upon termination of the Agreement, the Contractor is not entitled to any further payments hereunder.

5. Notices: Any notices required or permitted to be given pursuant to the terms of the Agreement must be in writing and either personally delivered or sent by nationally recognized overnight carrier to the parties at the following addresses:

To the Contractor:

Prentke Romich Company
1022 Heyl Rd.
Wooster, OH 44691
Attn: Legal
privacy@prc-saltillo.com

To the District:
Commack Union Free School District
PO Box 150
Commack, NY 11725
Attention: Superintendent of Schools

With a copy to:
Bond, Schoeneck, & King
225 Old Country Road
Melville, New York 11746
Attention: Eugene R. Barnosky, Esq.

If the notice is sent by personal mail, it will be deemed delivered upon receipt and if sent by registered or certified mail, it shall be deemed delivered 3 days after so mailing.

6. Modification: The Agreement may not be changed by any District Employee or other End User. The Agreement may not be changed orally, electronically, by click-through agreement, or by continued use. The Agreement may only be changed by an agreement in writing signed by the District. Any waiver of any term, condition or provision of the Agreement will not constitute a waiver of any other term, condition or provision, nor will a waiver of any breach of any term, condition or provision constitute a waiver of any subsequent or succeeding breach.

7. Governing Law, Choice of Forum and Waiver of Jury Trial: The Agreement is subject to, governed by, enforced according to and construed according to the laws of the State of New York, without regard to the conflicts of laws provisions thereof. Notwithstanding the arbitration provisions in the Contract, if any, the parties agree that any dispute arising under the Agreement will be litigated in a New York State Court in Suffolk County, New York. The parties each waive trial by jury in any action concerning the Agreement.

8. No Assignment: In accordance with the provisions of New York General Municipal Law § 109, the Contractor is hereby prohibited from assigning, transferring, conveying, subletting or otherwise disposing of the Agreement, or of the Contractor's rights, title, or interest in the Agreement, or the Contractor's power to execute the Agreement to any other person or corporation without the previous consent in writing from the District.

9. Third-Party Beneficiaries: There are no third-party beneficiaries in the Agreement.

10. Execution: This Rider may be executed in one or more counterparts, all of which

shall be considered one and the same agreement. This Rider may be executed by facsimile or PDF signature, each of which shall constitute an original for all purposes.

11. Notwithstanding the execution of this Rider or any other term or condition of this Rider, it will not become effective unless and until the Contract between the parties is in full force and effect.

IN WITNESS WHEREOF, the parties hereto have duly executed this Agreement.

Commack Union Free School District

By: _____

Alise Pulliam
Executive Director for Instructional Technology

Prentke Romich Company **, the Contractor**

By: Sandra Schleifer Digitally signed by Sandra Schleifer Date: 2024.10.31 15:17:12 -04'00'

Name: Sandra Schleifer
Title: Legal Director

EXHIBIT A

DATA PRIVACY AGREEMENT

COMMACK UNION FREE SCHOOL DISTRICT
DATA PRIVACY AGREEMENT

Between

COMMACK UNION FREE SCHOOL DISTRICT

and

Prentke Romich Company d/b/a PRC-Saltillo

This Data Privacy Agreement ("DPA") is by and between the Commack Union Free School District ("the District") and Prentke Romich Company ("the Contractor"), collectively, "the Parties."

ARTICLE I: DEFINITIONS

As used in this DPA, the following terms have the following meanings:

1. Breach: The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information of District Data, or a breach of the Contractor's security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personally Identifiable Information.

2. Commercial or Marketing Purpose: The sale, use or disclosure of Personally Identifiable Information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of Personally Identifiable Information for advertising purposes; or the sale, use or disclosure of Personally Identifiable Information to develop, improve or market products or services to students.

3. Disclose: To permit access to, or the release, transfer, or other communication of Personally Identifiable Information by any means, including oral, written or electronic, whether intended or unintended.

4. District Data: All information obtained by the Contractor from the District or by the Contractor in connection with the Services provided by the Contractor pursuant to the Service Agreement, including but not limited to business, administrative and financial data, intellectual property, student and personnel data, and metadata. The term, "District Data" does not include any information made publicly available by the District, except Personally Identifiable Information from student and personnel data which will be considered "District Data" regardless of whether or not it is made public.

5. Education Record: An education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.

6. Educational Agency: As defined in Education Law 2-d, a school district, board of cooperative educational services, School, or the New York State Education Department.

7. Eligible Student: A student who is eighteen years of age or older.

8. Encrypt or Encryption: As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR § 164.304, means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.

9. NIST Cybersecurity Framework: The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.

10. Parent: A parent, legal guardian or person in parental relation to the Student.

11. Personally, Identifiable Information ("PII"): Means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g, and Teacher or Principal APPR Data, as defined below.

12. Release: Has the same meaning as Disclose.

13. Service Agreement:

The agreement between the District and the Contractor with an effective date of July 1, 2022.

14. Services: The services provided by the Contractor to the District pursuant to the Service Agreement.

15. School: Any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law § 3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law § 4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.

16. Student: Any person attending or seeking to enroll in an Educational Agency.

17. Student Data: Personally, Identifiable Information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g. Personally Identifiable Information includes, but is not limited to: (i) a person's name or address or the names or addresses of a Student's parents or other family members; (ii) any personal identifier (*e.g.,* SSN, student number or biometric record); (iii) indirect identifiers (*e.g.,* date of birth, place of birth, or mother's maiden name); (iv) other information that alone or in combination is linked or linkable to a specific individual and would allow a reasonable person in the District community who does not have personal knowledge of the relevant circumstances to identify the individual with reasonable certainty; and (v) any information requested by a person who the District or the Contractor reasonably believes know the identity of the person to whom a record relates.

18. Subcontractor: The Contractor's non-employee agents, consultants and/or other persons or entities not employed by the Contractor who are engaged in the provision of Services pursuant to the Service Agreement.

19. Teacher or Principal APPR Data: Personally, Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to Release pursuant to the provisions of Education Law §§ 3012-c and 3012-d.

ARTICLE II: PRIVACY AND SECURITY OF PII

1. Compliance with Law.

In order for the Contractor to provide Services to the District pursuant to the Service Agreement; the Contractor may receive District Data regulated by several New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. § 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C.§§ 6501-6506 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. § 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. § 1400 et seq. (34 CFR Part 300); New York Education Law § 2-d; and the Commissioner of Education's Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements of New York law and to protect District Data. The Contractor agrees to maintain the confidentiality and security of District Data in accordance with applicable New York, federal and local laws, rules and regulations.

2. Authorized Use.

The Contractor has no property or licensing rights or claims of ownership to District Data, and the Contractor must not use District Data for any purpose other than to provide the Services set forth in the Service Agreement. The Contractor agrees that neither the Services provided to the District nor the manner in which the Services are provided by the Contractor will violate applicable New York, federal and local laws, rules and regulations.

If the Contractor has access to District Data that is subject to the Family Educational Rights and Privacy Act ("FERPA"), the Contractor acknowledges that for purposes of this Agreement it will be designated as a "school official" with a "legitimate educational interest" pursuant to FERPA and its implementing regulations, and the Consultant agrees to abide by the limitations and requirements imposed on school officials.

3. Collection of Data.

The Contractor represents and warrants that it will only collect data from the District or District employees or other End Users (the term "End Users" means the individuals authorized by the District to access and use the Services) that is necessary to fulfill the Contractor's duties pursuant to the Service Agreement.

4. Data Security and Privacy Plan.

The Contractor must adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect District Data in a manner that complies with New York, federal and local laws, rules and regulations and the District's policies. Education Law § 2-d requires that the Contractor provide the District with a Data Privacy and Security Plan that outlines such safeguards, measures and controls including how the Contractor will implement all applicable State, federal and local data security and privacy requirements. The Contractor's Data Security and Privacy Plan is attached to this DPA as Exhibit C and is incorporated into this DPA.

5. The District's Data Security and Privacy Policy

State law and regulation requires the District to adopt a data security and privacy policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST Cyber Security Framework. The Contractor represents and warrants that it will comply with the District's data security and privacy policy and other applicable policies.

6. Right of Review and Audit.

Upon request by the District, the Contractor will provide the District with copies of its policies and related procedures that pertain to the protection of PII and District Data. The policies and procedures may be made available in a manner that does not violate Contractor's own information security policies, confidentiality obligations, and applicable laws. In addition, Contractor may be required by the District to undergo an audit of Contractor's privacy and security safeguards, measures and controls as they pertain to alignment with the requirements of applicable New York, federal and local laws, rules and regulations, the District policies applicable to the Contractor, and alignment with the NIST Cybersecurity Framework performed by an independent third party at the Contractor's expense, and provide the written audit report to the District. The Contractor may provide the District with a recent industry standard audit report performed by an independent third party on the Contractor's privacy and security practices as an alternative to undergoing an audit. The determination of whether the previously prepared audit report is "recent" will be determined by the District in its sole judgment.

7. Access to/Disclosure of District Data

(a) The Contractor agrees that it will limit the Contractor's internal access to and only Disclose PII to the Contractor's officers, employees and Subcontractors who need to access the PII in order to provide the Services and that the disclosure of PII will be limited to the extent necessary to provide the Services pursuant to the Service Agreement. The Contractor must take all actions necessary to ensure that all its officers, employees and Subcontractors comply with the terms of this DPA.

(b) The Contractor must ensure that each Subcontractor performing functions pursuant to the Service Agreement where the Subcontractor will receive or have access to District Data must be contractually bound by a written agreement that includes confidentiality and data security obligations equivalent to, consistent with, and no less protective than, those found in this DPA.

(c) The Contractor must examine the data security and privacy measures of its Subcontractors prior to utilizing the Subcontractor to ensure compliance with this DPA. If at any point a Subcontractor fails to materially comply with the requirements of this DPA, the Contractor must: notify the District and prevent the Subcontractor's continued access to District Data; and, as applicable, retrieve all District Data received or stored by Subcontractor and/or ensure that District Data has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the Subcontractor compromises PII, the Contractor must follow the Data Breach reporting requirements set forth herein.

(d) The Contractor will take full responsibility for the acts and omissions of its officers, employees and Subcontractors.

(e) The Contractor must not Disclose District Data to any other party (a party other than the Contractor's officers or employees or Subcontractors who does not need access to the District Data to provide the Services pursuant to the Service Agreement) without the prior written consent of the District (if necessary, the District will obtain the required consent(s) from third parties) unless the disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the District of the court order or subpoena in advance of compliance but in any case, provides notice to the District no later than the time the District Data is disclosed, unless such disclosure to the District is expressly prohibited by the statute, court order or subpoena.

(f) Except as prohibited by law, the Contractor will: (i) immediately notify the District of any subpoenas, warrants, or other legal orders, demands or requests received by the Contractor seeking District Data; (ii) consult with the District regarding the Contractor's response; (iii) cooperate with the District's reasonable requests in connection with efforts by the District to intervene and quash or modify the legal order, demand or request; and (iv) upon the District's request, provide the District with a copy of the Contractor's response.

(g) Upon the District's request, the Contractor agrees that it will promptly make any District Data held by the Contractor available to the District.

8. Training.

The Contactor must ensure that all its officers, employees and Subcontractors who have access to PII have received or will receive training on the federal and State laws governing confidentiality of the data prior to receiving access.

9. Term and Termination.

This DPA will be effective as of the date the Service Agreement is effective and will terminate on the termination of the Service Agreement. However, the obligations of the parties pursuant to this DPA will survive the expiration of the Service Agreement and will continue until the Contractor and Subcontractors no longer retain PII and no longer retain access to PII.

10. Data Return and Destruction of Data.

(a) Protecting PII from unauthorized access and disclosure is of the utmost importance to the District, and the Contractor agrees that it is prohibited from retaining PII or continued access to PII or any copy, summary or extract of PII, on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever beyond the period of providing Services to the District, unless such retention is expressly authorized for a prescribed period by the Service Agreement or other written agreement between the Parties, expressly requested by the District for purposes of facilitating the transfer of PII to the District or expressly required by law. As applicable, upon expiration or termination of

the Service Agreement, the Contractor will transfer PII, in a format agreed to by the Parties to the District.

(b) If applicable, once the transfer of PII has been accomplished in accordance with the District's written election to do so, the Contractor agrees to return or destroy all PII when the purpose that necessitated its receipt by the Contractor has been completed. Thereafter, with regard to all PII (including without limitation, all hard copies, archived copies, electronic versions, or electronic imaging of hard copies) as well as any and all PII maintained on behalf of the Contractor in a secure data center and/or in cloud-based facilities that remain in the possession of the Contractor or its Subcontractors, the Contractor will ensure that PII is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed. Hard copy media must be shredded or destroyed such that PII cannot be read or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. Only the destruction of paper PII, and not redaction, will satisfy the requirements for data destruction. Redaction is specifically excluded as a means of data destruction.

(c) The Contractor will provide the District with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.

(d) To the extent that the Contractor and/or its Subcontractors continue to be in possession of any de-identified data (*i.e.,* data that has had all direct and indirect identifiers removed), the Contractor agrees not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

11. Commercial or Marketing Use Prohibition.

Contractor agrees that it will not sell PII or use or Disclose PII for a Commercial or Marketing Purpose.

12. Encryption.

The Contractor will use industry standard security measures including Encryption protocols that comply with New York law and regulations to preserve and protect PII. Contractor must Encrypt PII at rest and in transit in accordance with applicable New York laws and regulations.

13. Storage.

Contractor must store all District Data within the United States of America.

14. Breach.

a. The Contractor must promptly notify the District of any Breach of PII in the most expedient way possible and without unreasonable delay and in no event more than seven calendar days after discovery of the Breach. Notifications required pursuant to this section must be in writing and by email (if email address is provided) and personal delivery or nationally recognized overnight carrier. Notifications must to the extent available, include a description of the Breach which includes the date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Contractor's investigation; and the contact information for

representatives who can assist the District. Violations of the requirement to notify the District are subject to civil penalty(ies) pursuant to Education Law § 2-d. The Breach of certain PII protected by Education Law §2-d may subject the Contractor to additional penalties.

b. Notifications required to be made to the District pursuant to this paragraph must be sent to the following people at the following addresses:

Dr. Jordan Cox
Superintendent of Schools
Commack Union Free School District
PO Box 150
Commack, NY 11725
Email: jcox@commack.k12.ny.us

Mrs. Alise Pulliam
Executive Director for Instructional Technology
Commack Union Free School District
PO Box 150
Commack, NY 11725
Email: apulliam@commack.k12.ny.us

15. Cooperation with Investigations.

Contractor agrees that it will cooperate with the District and law enforcement, where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Contractor or its' officers, employees or Subcontractors, as related to such investigations, will be the sole responsibility of the Contractor if the Breach is attributable to Contractor or its Subcontractors.

16. Notification to Individuals.

Where a Breach of PII occurs that is attributable to Contractor, Contractor will pay for or promptly reimburse the District for the full cost of the District's notification to Parents, Eligible Students, teachers, and/or principals, in accordance with Education Law § 2-d and 8 NYCRR Part 121.

ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS

1. Parent and Eligible Student Access.

Education Law § 2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student's Student Data stored or maintained by the District. To the extent Student Data is held by the Contractor pursuant to the Service Agreement, the Contractor must respond within 20 calendar days to the District's requests for access to Student Data so the District can facilitate review by a Parent or Eligible Student, and facilitate corrections, as necessary. If a Parent or Eligible Student contacts Contractor directly to review any of the Student Data held by the Contractor pursuant to the Service Agreement, the Contractor must promptly notify the District and refer the Parent or Eligible Student to the District.

2. Bill of Rights for Data Privacy and Security.

As required by Education Law § 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Service Agreement are annexed hereto as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. The Contractor must complete and sign Exhibits A and B. Pursuant to Education Law § 2-d, the District is required to post the completed Exhibit B on its website.

ARTICLE IV: MISCELLANEOUS

1. Priority of Agreements and Precedence.

In the event of a conflict between and among the terms and conditions of this DPA, including all Exhibits attached hereto and incorporated herein and the Service Agreement, the terms and conditions of this DPA will govern and prevail, will survive the termination of the Service Agreement in the manner set forth herein, and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto.

2. Execution.

This DPA may be executed in one or more counterparts, all of which will be considered one and the same document, as if all parties had executed a single original document, and may be executed utilizing an electronic signature and/ or electronic transmittal, and each signature thereto will be and constitute an original signature, as if all parties had executed a single original document.

Commack Union Free School District	
By: (Signature)	By: (Signature) Sandra Schleifer Digitally signed by Sandra Schleifer Date: 2024.10.31 15:16:54 -04'00'
Alise Pulliam	(Printed Name) Sandra Schleifer
Executive Director for Instructional Technology	(Title) Legal Director
Date: 11/13/2025	Date: 10/31/2024

EXHIBIT A - Education Law § 2-d Parents' Bill of Rights for Data Privacy and Security

COMMACK UNION FREE SCHOOL DISTRICT

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY –

Summary of Rights and Information for Parents and Students

The legislature and governor passed a group of bills that adjusted the Regents Education Reform Agenda. These bills are known collectively as the "Common Core Implementation Reform Act." One of the key components of this act (Chapter 56, Part AA, Subpart L, of the laws of 2014) directs the Commissioner of Education to appoint a Chief Privacy Officer (CPO). A major function of this new position is to work with school districts and parents to develop elements for a parents' bill of rights to help ensure that student data is private and secure. The State Education Department (SED) and the CPO must also recommend regulations to establish standards for data security and privacy policies that will be implemented statewide.

SED has issued a preliminary Parents' Bill of Rights for Data Privacy and Security. The Commack Union Free School District is issuing this summary of parents' rights under the new law. While some additional elements will be developed in conjunction with the CPO, districts, parents and the Board of Regents, this summary sets forth the key rights and information that parents should be aware of in regards to ensuring the privacy and security of their student's educational data.

The Commack Union Free School District is committed to ensuring student privacy and recognizes that parents, legal guardians, and persons with a parental relationship to a student are entitled to certain rights with regard to their child's personally identifiable information, as defined by Education Law §2-d. To this end, the District is providing the following Parent's Bill of Rights for Data Privacy and Security:

1. A student's personally identifiable information cannot be sold or released for any commercial purposes;

2. Parents have the right to inspect and review the complete contents of their child's education record;

3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred;

4. A complete list of all student data elements collected by the State is available for public review at http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx or by

writing to the Office of Information & Reporting Services, New York State Education Department, Room 863, 89 Washington Avenue, New York 12234; and

5. Parents and guardians have the right to have complaints about possible breaches of student data addressed. Complaints should be addressed to Alise Pulliam, Executive Director for Instructional Technology, PO Box 150, Commack, New York 11725, Phone: (631) 912-2027, Email: alisepulliam@commack.k12.ny.us or Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234.

If the Commack Union Free School District enters into a third-party contract in which the service provider receives student data or teacher or principal data in order to provide a needed service for the District, supplemental information shall be developed and provided to parents that states:

6. The exclusive purposes for which the student data or teacher or principal date will be used;

7. How the third-party contractor will ensure that the subcontractors, persons or entities that the third-party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;

8. When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement;

9. If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; and

10. Where the student data or teacher or principal data will be stored and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

The CPO as appointed by the Commissioner must secure input from parents and other education and expert stakeholders to develop additional elements for the Parents' Bill of Rights for Data Privacy and Security. The Commissioner of Education will also be promulgating regulations with a comment period for parents and other members of the public to submit comments and suggestions to the CPO.

In the meantime, you can access additional information and a question and answer document issued by SED as a preliminary Parents' Bill of Rights for Data Privacy and Security.

If you have any further questions or concerns at this time, please contact Dr. Jordan Cox, Superintendent, Commack UFSD, PO Box 150, Commack, New York 11725 or Mrs. Alise Pulliam at apulliam@commack.k12.ny.us

By: (Signature) Sandra Schleifer Digitally signed by Sandra Schleifer Date: 2024.10.31 15:16:37 -04'00'
(Printed Name) Sandra Schleifer
(Title) Legal Director
Date: 10/31/2024

EXHIBIT B: BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY -

SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

Pursuant to Education Law § 2-d and 8 NYCRR § 121.3, the District is required to post information to its website about its contracts with third-party contractors ("Service Agreements") that will receive Personally Identifiable Information ("PII") from Student Data or Teacher or Principal APPR Data.

Term of Service Agreement	Agreement Start Date: October 1st, 2024 Agreement End Date: June 30th, 2027
Description of the purpose(s) for which Contractor will receive/access/use PII	PII received by the Contractor will be received, accessed and used only to perform the Contractor's Services pursuant to the Service Agreement with the District. List Purposes: No PII will be received for the performance of the Agreement. PRC-Saltillo does not receive or process PII with the use of NuVoice PASS or ChatEditor software.
Type of PII that Contractor will receive/access	Check all that apply: ☐ Student PII ☐ Teacher or Principal APPR Data
Subcontractor Written Agreement Requirement	The Contractor will only share PII with entities or persons authorized by the Service Agreement. The Contractor will not utilize Subcontractors without written contracts that require the Subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Service Agreement. Check applicable option. ☑ Contractor will not utilize Subcontractors.

	☐ Contractor will utilize Subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Service Agreement, the Contractor will, as directed by the District in writing: • Securely transfer data to District, or a successor contractor at the District's option and written discretion, in a format agreed to by the parties. • Securely delete and destroy data by taking actions that render data written on physical (e.g., hard copy) or electronic media unrecoverable by both ordinary and extraordinary means.
Challenges to Data Accuracy	Parents, students, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the District. If a correction to data is deemed necessary, the District will notify the Contractor. The Contractor agrees to facilitate such corrections within 21 calendar days of receiving the District's written request.
Secure Storage and Data Security	The Contractor will store and process District Data in compliance with § 2-d(5) and applicable regulations of the Commissioner of Education, as the same may be amended from time to time, and in accordance with commercial best practices, including appropriate administrative, physical and technical safeguards, to secure district Data from unauthorized access, disclosure, alteration and use. The Consultant will use legally-required, industry standard and up-to-date security tools and technologies such as anti-virus protections and intrusion detection methods in providing services pursuant to the Service Agreement. The Contractor will conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner. Please describe where PII will be stored and the security protections taken to ensure PII will be protected and data security and privacy risks mitigated in a manner that does not compromise the security of the data: (a) Storage of Electronic Data (check all that apply): ☐ Using a cloud or infrastructure owned and hosted by a third party. ☐ Using Contractor owned and hosted solution

	☐ Other: N/A, no PII will be stored (b) Storage of Non-Electronic Data: N/A (c)Personnel/Workforce Security Measures: PRC-Saltillo uses KnowBe4 trainings that are required for all personnel on a regular basis consistent with all regulations. PRC-Saltillo also runs phish testing on all users every 2 weeks and requires remedial training for those who fail. (d) Account Management and Access Control: PRC-Saltillo has a logical access policy that can be provided upon request (e) Physical Security Measures: PRC-Saltillo has a physical access policy that can be provided upon request (f) Other Security Measures:
Encryption	Data will be encrypted while in motion and at rest.

By: (Signature) Sandra Schleifer Digitally signed by Sandra Schleifer Date: 2024.10.31 15:16:24 -04'00'
(Printed Name) Sandra Schleifer
(Title) Legal Director
Date: 10/31/2024

EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Commack Union Free School District is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. The Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York State. The terms of the plan cannot conflict with any other terms of or Exhibits to the Data Privacy Agreement to which this Exhibit C is attached. **While this plan is not required to be posted to the District's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems. DO NOT LIMIT RESPONSES TO THE SPACES PROVIDED.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract	Identified contractual requirements will be reviewed and reasonably implemented and maintained through the life of the contract
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Employee confidentiality training, process in place to check for and identify data breaches, and written plan in place for security incidents.
3	Specify how your officers, employees and Subcontractors who have access to PII pursuant to the Service Agreement will receive training on the federal and State laws that govern the confidentiality of PII.	Employees are trained on data privacy upon hire and training is updated on a yearly basis.
4	Outline the processes that ensure that your officers, employees and Subcontractors are bound by written agreement to the requirements of the Service Agreement, at a minimum.	Each employee is bound by a confidentiality agreement.
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the District.	PRC-Saltillo has an incident and breach response policy that can be provided upon request.

6	Describe how data will be transitioned to the District when no longer needed by you to meet your contractual obligations, if applicable.	No PII is collected.
7	Describe your secure destruction practices and how certification will be provided to the District.	No PII is collected.
8	Outline how your data security and privacy program/practices align with the District's applicable policies.	PRC-S maintains several policies and can provide upon request. Policies include: Logical Access IT Encryption Incident and Breach Response Electronic Communication and Usage
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	***YOU MAY USE TEMPLATE BELOW***

EXHIBIT C.1 – NIST CSF TABLE

The table below will aid the review of a Contractor's Data Privacy and Security Plan. Contractors should complete the Contractor Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. To complete these 23 sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-7 ; (ii) Use a narrative to explain alignment (may reference its applicable policies); and/or (iii) Explain why a certain category may not apply to the transaction contemplated. Further informational references for each category can be found on the NIST website at https://www.nist.gov/cyberframework/new-framework. Please use additional pages if needed.

Function	Category	Contractor Response
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	PRC-Saltillo uses Connectwise to manage software, systems, devices, and facilities. We have multiple systems that manage data.
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions	PRC-Saltillo is a mission based company as well as a health care provider. A current company goal is to focus on the privacy and security of our client information and the implementation of privacy by design.
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	PRC-Saltillo is ISO 9001 certified and have these documented in that process and that informs us on the cybersecurity side for what we need to be following and pay attention to.
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	PRC-Saltillo has formally appointed HIPPAA Privacy and Security Officers. The Privacy and Security Officers fully understand the risk to organization operations, assets, and individuals.
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	PRC-Saltillo has a known and understood risk management strategy.

PROJECT (PR)	**Supply Chain Risk Management (ID.SC):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	PRC-Saltillo uses reputable suppliers.
	Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	PRC-Saltillo uses physical and logical access controls in which only specific personnel have access to make changes.
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	PRC-Saltillo uses KnowBe4 trainings that are required for all personnel on a regular basis consistent with all regulations. PRC-Saltillo also runs phish testing on all users every 2 weeks and requires remedial training for those who fail.
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	Yes, the confidentiality and security of data is a company priority.
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	Incident and Breach Response policy is published. Incident Response and Disaster Recovery are drafted and awaiting publication.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	Yes, all maintenance and repairs are done according to strict security protocols. When an outside contractor needs to do the work an IT staff member supervises the whole time.
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	Yes, all technical security solutions are kept up to date and checked regularly for alternations or intrusions.
	Anomalies and Events (DE.AE):	

DETECT (DE)	Anomalous activity is detected and the potential impact of events is understood.	Privileged access is audited quarterly.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	Trend VisionOne in place on all workstations, laptops, and windows servers.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Trend VisionOne in place on all workstations, laptops, and windows servers.
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	Incident and Breach Response policy is published.
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	Yes, a breach policy is in place.
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	We maintain cybersecurity insurance and auditing in response to a breach is part of our coverage.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Yes
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Yes, we always do a post mortem and make changes accordingly.
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	Disaster Recovery policy is drafted and awaiting publication.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	Yes
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	Yes

ELECTRONIC COMMUNICATIONS POLICY

Overview

PRC uses many forms of electronic communication, media and services, including computers, e-mail, phones, voice mail, fax, on-line services, web sites, social networking sites and the internet. PRC encourages the use of electronic media to better serve our customers and provide our talented workforce with the best tools to do their jobs.

Electronic media and services provided by the company are company property and their purpose is to facilitate and support company business. They are not the private property of any employee. Employees should have no expectation of privacy with respect to any usage of the company's electronic communication systems and equipment.

Rules cannot be established to cover every possible situation; therefore this policy is designed to express PRC's philosophy and set forth general practices and use of electronic media and services by employees. The following procedures apply to all electronic media and services that are:

- Accessed on or from company premises;
- Accessed using company computer equipment or via company-paid access methods;
- Used in a manner that identifies the individual with the company.

Computer/Software Use

PRC must have a clear license, right to use and/or ownership for all software installed on PRC computers and media downloaded from the internet. Software purchased by you personally may not be installed on PRC computers. Software downloaded from the internet (shareware or freeware) should be approved by a system administrator prior to installation on a PRC computer. All software that is downloaded or installed should be work related.

Data

Data is defined as all recorded information, electronic or otherwise used to conduct PRC business, including, but not limited to: customer information, product information, marketing materials, development materials and education and training materials.

PRC owns all data created or collected by its employees or contractors, except when the creation or collection of such data is governed by a written agreement or contract stating otherwise.

PRC data may not be stored on employee's personal electronic devices. Upon termination of employment, data remains the property of PRC and all data (original and copies) must be returned to PRC.

Internet/Network Use

A limited amount of bandwidth is available for all employees to share. Excessive bandwidth use, can cause delays for all employees. The following types of personal activities use an excessive amount of bandwidth, and are prohibited:

- Listening to Internet Radio or streaming videos or movies (such as: YouTube, Pandora, or other like activities)
- Downloading music files, large image, data or video files, screensavers or sound clips
- Installation of software that maintains an internet connection and uses excess bandwidth
- Downloading application files for personal use

PRC recognizes that employees with laptops will connect to the Internet from their home. All employees who use a home connection must coordinate with PRC's IT department to ensure that connection is secure. All employees who maintain a primary office in their home and have PRC funded Internet service, must coordinate changes to the Internet Service Provider with PRC's IT department. In-home wireless access is not permitted. Please refer to the paragraph on Wireless Communication for details.

Prohibited Communication
When using PRC equipment or posting on or to PRC-related social media or other venues, such electronic media shall not be used for knowingly transmitting, retrieving, viewing, accessing, or storing any communication that may be considered:

- Discriminatory or harassing, obscene, defamatory or threatening, or derogatory to any individual or group based on race, sex, religion, national origin, disability or other protected classifications; or
- Engaged in for any purpose that is illegal or contrary to PRC's policy or business interests; or
- Inconsistent with PRC's established brand and use text descriptions and imagery, as provided and approved by PRC's Marketing staff. Employees may not express clinical opinions or other representations that are not consistent with PRC's corporate message and image when representing PRC in any fashion. If ever an employee has a question or concern about a communication he/she plans to make, please review it with your supervisor and PRC's Marketing staff.

Personal Use
Electronic media and services are provided by PRC primarily for employees' business. Limited, occasional, or incidental use of electronic media (sending or receiving) for personal, non-business purposes is permitted. However, employees are expected to demonstrate a sense of responsibility and not abuse this privilege. Subscription to personal e-mail lists resulting in large volumes of mail is not appropriate.

Access to Employee Communications
PRC reserves the right to monitor any electronic or telephonic communications conducted on or over PRC owned devices on or using PRC funded equipment. Additionally, the following conditions should be noted:

Individual use patterns—for example, telephone numbers dialed, sites accessed, call length, and time at which calls are made—can be monitored for the following purposes:

- Cost analysis;
- Resource allocation;
- Optimum technical management of information resources; and
- Detecting patterns of use that indicate employees are violating PRC policies or engaging in illegal activity.

PRC reserves the right, at its discretion, to review any employee's electronic files and messages to the extent necessary to ensure electronic media and services are being used in compliance with the law, this policy, and other PRC policies.

Employees should have no expectation of privacy in any messages, files or information composed, sent, contained/stored or received via the company's electronic communications systems and equipment.

Accordingly, if an employee transmits sensitive personal information he/she is encouraged to use other, more private means, such as a personal telephone.

Security/Appropriate Use
Employees must respect the confidentiality of other individuals' electronic communications. Except in cases in which explicit authorization has been granted by company Management, employees are prohibited from engaging in, or attempting to engage in:

- Monitoring or intercepting the files or electronic communications of other employees or third parties;
- Cracking or obtaining access to systems or accounts they are not authorized to use;
- Using other people's log-ins or passwords; and
- Breaching, testing, or monitoring computer or network security systems.

No e-mail or other electronic communications may be sent that attempts to hide the identity of the sender or represent the sender as someone else. Unless authorized by the Management Team, users may not send unsolicited commercial e-mail or other electronic messages regardless of its appropriateness to PRC business except in forums specifically created for this purpose.

Electronic media and services should not be used in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system.

Anyone obtaining electronic access to other companies' or individuals' materials must respect all copyrights and may not copy, retrieve, modify, or forward copyrighted material except as permitted by the copyright owner.

Customer Credit Card
Some employees will have access to customer credit card information. Credit card information may be received electronically, by fax, mail or phone. Only authorized employees are permitted to access this information. Employees must respect the confidentially of credit card information and keep it secure at all times. Once the credit card information is no longer needed, it must be disposed of properly.

If an employee learns that customer credit card information has been compromised either electronically or in paper format, the Security Response Team must be notified immediately. The Security Response Team is the IT Department and Director of Finance.

Please refer to the Credit Card Policy and Security Incident Response Procedure on the following pages for additional details.

Wireless Communication
PRC recognizes the need for employees to demonstrate PRC products (such as the Support knowledgebase or the Language Lab) adequately and to utilize the convenience of a wireless connection. Wireless Internet Access can be difficult to secure. Employees must be mindful of the risks involved in using wireless and exercise caution when doing so. PRC requires use of a wired connection to the internet whenever possible.

Under the following circumstances wireless access is allowed. From a hotel, an airport or at a conference or facility, an employee may use wireless access with the wireless card in his/her computer. Wireless access points in corporate environments are assumed to be relatively secure where an IT staff is responsible for managing the wireless network. However, even in these environments, wireless

connections can be hacked and data packets can be intercepted so it is strongly suggested that an employee not use a wireless connection for any banking or credit card transactions.

DO NOT, under any circumstances, use an employee PRC VISA card for any transactions while using a wireless connection. A company credit card should only be used when an employee is connected to the internet by a hard wired connection. Violation of this policy will result in revocation of credit card privileges.

A WLAN (wireless local area network) from home is not secure. An in-home Wireless connection requires the same level of attention and maintenance from an IT professional as a commercial environment to be secure. The cost of securing an in-home wireless network for each employee with a home office far outweighs the benefits experienced by having it. Therefore, employees are NOT permitted to setup a wireless router or any type of wireless access point to a PRC funded DSL or cable connection at home. Also, employees are NOT permitted to connect a PRC laptop to a personal home network that allows wireless access. (WLAN)

Occasionally, personal circumstances may arise where exceptions are made to this policy. Any exceptions to this policy will be reviewed on a case by case basis and must be discussed and approved by PRC IT staff.

Encryption
Employees shall use encryption software supplied to them by the systems administrator for purposes of safeguarding sensitive or confidential business information. Employees who use encryption on files stored on a company computer must provide their supervisor with a sealed hard copy record (to be retained in a secure location) of all of the passwords and/or encryption keys necessary to access the files.

Participation in Social Media and Web Communication Sites
Employees have an opportunity to express themselves and communicate online in many ways and PRC encourages an online presence. Employees must be professional, ethical, and respectful and use good judgment in their online communications. This section will set forth guidelines that employees should follow for all online communications in reference to PRC.

This policy includes, but is not limited to, the following specific technologies:

- Personal blogs, web sites and news groups
- Professional blogs, web sites, news groups and list serves
- LinkedIn
- Twitter
- Facebook
- My Space
- Wikipedia

Any material posted online in reference to PRC is the responsibility of the poster. The communication should be made in a manner that identifies credibility. An employee must state that the opinion is his/hers individually and is not a form of official communication from PRC. Communication should be relevant to your area of expertise, professional, honest and respectful. The communication should not "leak" information, share financial information or trade secrets, customer data, and intellectual property or make inaccurate, distasteful or defamatory comments about PRC.

Statements about PRC, including but not limited to, the company, products, services, and employees, that are inconsistent with the established brand image and/or approved text descriptions and imagery provided by PRC Marketing staff are prohibited. If ever an employee has a question or concern about a communication he/she plans to make, please review it with his/her supervisor and PRC's Marketing staff.

If an employee becomes aware of social networking activity that is deemed distasteful, inaccurate or shares financial information, trade secrets, customer data and/or intellectual property, the employee has a duty to contact the IT department immediately.

Some social sites such as LinkedIn allow members to recommend current or former co-workers. PRC does not permit employee recommendations for reasons of company liability.

Employees signing up for sites agree to abide by the Terms of Service (TOS) for that site. Employees are responsible to read, know and comply with the TOS of sites used.

Employees must have written permission from PRC's Marketing Department before setting up PRC branded professional sites, groups and/or pages. Postings and profiles should not include corporate logos, unless authorized by PRC's Marketing Department. Employees must comply with the law in regard to copyright and plagiarism at all times.

While social networking can be a useful tool for developing business relationships, it can also impact productivity. Social networking activities should not interfere with the employee's primary job responsibilities.

Nothing in this policy will be construed or applied in a manner that interferes with employees' rights to communicate with their fellow employees about terms and conditions of employment.

Policy violations
Employees who abuse the privilege of company-facilitated access to electronic media or services are subject to corrective action and risk having the privilege removed for themselves and possibly other employees. Violation of these policies can result in disciplinary action, up to and including termination.

Electronic Communications and Use Policy

I have read and understand the Electronic Communications and Use Policy.

_____ _____

Employee Name and Signature Date

PRC-Saltillo Encryption Policy

Contents

Introduction

Purpose

This policy was established to provide a guideline that will ensure that PRC-Saltillo will properly handle data in transit and at rest depending on the classification.

Scope

This policy applies to PRC-Saltillo's physical and virtual assets and anyone handling PRC-Saltillo data and equipment.

Disclaimer

If any employee is unclear about the nature of this policy or unsure if they are in violation of this policy, it is their responsibility to reach out to their department leader to contact the IT Security Officer.

Definition

Data at Rest

Data at rest refers to data residing in computer storage in any digital form. This data type is currently inactive and is not moving between devices or two network points. No app, service, tool, third-party, or employee is actively using this type of info.

At rest is not a permanent data state. As soon as someone requests a file, that data moves across a network and becomes in-transit data. Once someone (or something) starts processing a file, the data enters the in-use state.

Data at rest includes both structured and unstructured data. Some examples of where a company can store data at rest are:

- Hard and SSD drives on PCs and laptops.
- Database Servers
- The cloud.
- At a third-party colocation facility.
- Edge-point devices and portable storage (mobile phones, USBs, tablets, portable hard drives, etc.).
- Network-attached storage (NAS).

Data in Transit

Data in transit (also known as data in motion or flight) is a piece of data actively moving between two network locations. Being in transit is one of the three primary states of data (the two others are at rest and in use). Here are a few examples of a file in transit:

- Sending an email over the Internet.
- Two employees exchanging files over a corporate network.
- Sending a message over an instant messenger (like WhatsApp or Viber) or a collaboration platform (like Slack or Microsoft Teams).
- Uploading a file from local storage to a cloud computing environment (or vice versa).
- Transferring data from a USB to a coworker's personal laptop.
- IoT data traveling between the cloud and an edge server.
- Data moving between a web app and a browser.
- Data traveling between different cloud deployment models within a multi-cloud strategy.

There are two broad categories of data in transit:

- Data flowing over public or untrusted networks (the Internet being the most common example).
- Files flowing within the confines of a private network (such as a corporate local area network (LAN)).

Policy

PRC-Saltillo Employees are responsible for the physical security of any devices containing confidential and/or protected information and must report any device that is lost or stolen as soon as it is possible.

Storage (Encryption at Rest)

All electronic devices which receive, store, and/or transmit protected information must use PRC-Saltillo approved encryption methods that comply with applicable laws and regulations to secure the information stored or transmitted outside PRC-Saltillo.

- Servers that are not located at PRC-Saltillo's Headquarters are required to have all information stores of protected information encrypted.
- Servers at PRC-Saltillo Headquarters contain information of various classes and are accessed via public networks shall have protected information encrypted.
- Protected information contained on laptops or workstations are required to be encrypted – file, folder, or full disk.
- Files will be encrypted prior to storage on devices that are not able to be encrypted.
- Any and all mobile devices (e.g. smart phones and tablets) that connect to PRC-Saltillo's internal network that may contain or transmit protected information are required to accept information security standards to encrypt and protect the devices.
- External storage media (e.g. backup tapes, removable drives, etc.) are required to have Protected Information encrypted.
- Encryption will not be removed or disabled from any device without the approval of the IT Department.

Existing systems and applications containing protected information which cannot use encryption because of technology limitation, but have compensating controls, may be granted a special exception by the IT Department. However, these systems and applications will be required to have a formal risk assessment performed by IT to ensure that major risks are addressed via compensating controls to protect the data in lieu of encryption. Exceptions will be reviewed periodically and removed when a suitable solution is available.

Transmission (Encryption in Transit)

To ensure the confidentiality and integrity of protected information PRC-Saltillo will implement technical security measures to guard against unauthorized exposure of protected information during transmission on internal network or to an external location.

- Files that contain protected information that are transmitted across the Internet (e.g. email attachments sent to non-PRC-Saltillo addresses, or file transfers to other entities) will need to have the attachments encrypted or use a PRC-Saltillo secure encrypted method to deliver that information.
- All transmissions of protected information across public infrastructures including, but not limited to, personal email accounts, public cloud services, vendor systems, must either encrypt the information or encrypt the connection between the sending and the receiving entity.
- All transmissions of protected information across public networks must also ensure the integrity of protected information that it is not improperly modified without detection while in transit.
- PRC-Saltillo Employees are responsible for ensuring an approved method is used to transmit PRC-Saltillo information that has been classified as requiring encryption.

PRC-Saltillo employees, contractors, volunteers, contractors, and interns that are responsible for the transmission of protected information will follow the Transmission Security Standard and Encryption

Standard to ensure a secure mechanism will be used to transmit the information. If not able to meet the requirements, an exception may be requested from the IT Department.

Policy Compliance

The IT Department will measure compliance to this policy through various methods, including, but not limited to – reports, internal/external audits, and feedback to the policy owner. Exceptions to the policy must be approved by IT in advance. Non-compliance will be addressed with Leadership, IT Security Officer, Human Resources, or the Legal and Compliance Department.

Related Policies

- IT Sanctions Policy
- HIPAA Compliance Manual
- Electronic Communications Policy
- Data Classification Policy

Distribution, Violations, and History

Distribution

This policy should be available to all PRC-Saltillo employees and partners handling company data and PRC-Saltillo staff responsible for data support.

Policy Violations

Violations to this policy will result in disciplinary action, up to and including termination of employment or services.

Policy Version History

Version	Date	Description	Approved By
1.0	09/14/2023	Initial Policy Drafted	Joe Hartman

PRC-Saltillo
Security Policy

Access Control

Version 1.0
March 30, 2023

Document Revision History

Date	Version	Description	Author
3/30/2023	1.0	Published AC Policy	Joe Hartman (IT Security Officer)

Table of Contents

1 INTRODUCTION

PRC-Saltillo has developed corporate policies that identify the security requirements for its information systems and personnel to ensure the integrity, confidentiality, and availability of its information. These policies are set forth by PRC-Saltillo management and in compliance with the Access Control family of controls found in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4.

2 PURPOSE

The purpose of these policies is to establish access control requirements to ensure the confidentiality, integrity, and availability of PRC-Saltillo systems, facilities, and data are protected. These policies are consistent with applicable state and federal laws, Executive Orders, directives, regulations, standards, and guidance.

3 SCOPE

The provisions of these policies pertain to all PRC-Saltillo employees, contractors, third parties, and others who have access to company and customer confidential information within PRC-Saltillo systems and facilities.

4 ROLES AND RESPONSIBILITIES

These policies apply to all PRC-Saltillo employees, contractors, business partners, third parties, and others who need or have access to PRC-Saltillo systems and our customer's confidential information.

Dave Hershberger	CEO	Highest-level official with overall responsibility to develop, implement, and maintain accountability, active support, oversight, and management commitment for information security objectives.
Business Process Owners (Business Process Owners are in the process of being defined. 1-4-2024)	Information Owner	Has statutory, management, or operational authority for PRC-Saltillo information within the scope of their business process. Responsible for developing, implementing, and maintaining policies and procedures governing information generation, collection, processing, dissemination, and disposal.
IT Dept	Authorizing Official	Responsible for operating information system at an acceptable level of risk to organizational operations and assets.
IT Dept/Eng	Authorizing Official Designated Representative	Acts on behalf of Authorizing Official to coordinate and conduct day-to-day activities associated with security authorization process.
Reid Gerber	Information Technology Director	Responsible for the procurement, development, integration, modification, operation,

		maintenance, and disposal of an information system.
Joe Hartman	Information System Security Officer	Responsible for ensuring that the appropriate operational security posture is maintained for an information system, responsible for ensuring coordination among groups is managed and maintained for these policies/procedures. Responsible for conducting information system security engineering activities. Responsible for providing for appropriate security, to include management, operational, and technical controls.
David Casey	System Administrator	Responsible for conducting information system security administration activities.
ALL PRC-Saltillo Managers	Managers	Responsible for understanding, enforcing, and complying with control requirements defined in Policies and Procedures
Everyone Involved with PRC-Saltillo Information	Users of PRC-Saltillo Information Systems	Responsible for understanding and complying with Policies and Procedures.

5 MANAGEMENT COMMITMENT

PRC-Saltillo and its management are fully committed to protecting the confidentiality and integrity of corporate proprietary and production systems, facilities, and data as well as the availability of services in the PRC-Saltillo system by implementing adequate security controls.

6 AUTHORITY

These policies and procedures are issued under the authority of the PRC-Saltillo Information Owner. The following applicable laws, directives, policies, regulations, and standards were used as part of the development for this policy. These include, but are not limited to:

1. E-Government Act of 2002/Federal Information Security Management Act of 2002 (FISMA)
2. The Privacy Act of 1974
3. Clinger-Cohen Act of 1996
4. OMB Circulars and Memoranda
5. Federal Information Processing Standards (FIPS)
6. NIST Special Publications
7. OMB Memorandum for Chief Information Officers and Chief Acquisition Officers: Ensuring New Acquisitions Include Common Security Configurations, June 2007

8. OMB Memorandum for Agency CIOs: Security Authorization of Information Systems in Cloud Computing Environments, December 2011
9. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

7 COMPLIANCE

Compliance with these policies is mandatory. It is PRC-Saltillo's policy that information systems meet or exceed the requirements outlined in this document. The Information Owner will periodically assess compliance with these policies by using an independent audit performed annually by an external vendor to identify areas of non-compliance. Any findings identified in the audit will be remediated in accordance with the auditing team's recommendations.

8 POLICY REQUIREMENTS

The following access control requirements, mechanisms, and provisions are to be followed by all employees, management, contractors, and other users who access and support the PRC-Saltillo information systems.

8.1 ACCESS CONTROL POLICIES AND PROCEDURES

This document is intended to serve as the *Access Control Policy* and is made available to all applicable personnel. The associated procedure(s) to facilitate the implementation of the *Access Control Policy* and related physical and environmental protection controls have been developed, documented, and disseminated to all applicable personnel.

The Information Owner will review and update the *Access Control Policy* every three (3) years and the procedure(s) at least annually or any time there are significant changes in software or security. Updates must be made to keep the policy and procedure(s) in alignment with PRC-Saltillo's overall business goals and risk position. Any updates, improvements, or suggestions regarding the *Access Control Policy* and/or procedure(s) must be sent to the Information Owner.

8.2 ACCOUNT MANAGEMENT

PRC-Saltillo has implemented and maintains an information system account management process intended to carry out the following activities:

1. Identify accounts necessary to support company mission and business functions including Individual, Group, System, Application, Guest/Anonymous, Temporary, and other accounts if they exist
2. Establish conditions for group and role membership
3. Control information system access, employing group and role membership, access authorizations, and defined attributes for each account
4. Ensure all information system accounts require approval by defined personnel or roles
5. Maintain the capability to establish, activate, modify, disable, or remove accounts in accordance with defined policies and procedures
6. Monitor information system account users

7. Ensure mechanisms are implemented to notify account managers when accounts are no longer required, including when information system users are terminated transferred, or information system usage or need-to know/need-to-share changes
8. Grant information system access based on a valid access authorization, intended system usage, and company defined attributes
9. Ensure system accounts are reviewed annually
10. Employ a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group
11. Employ automated mechanisms to support in the management of information system accounts, including those identified in AC-2(a)
12. Have mechanisms in place to automatically remove or disable temporary and emergency accounts after no more than thirty (30) days
13. Require users to log out when they expect to be away from their workstations for a defined period of time in accordance with a defined time period of expected inactivity or a description of when to log out
14. Establish and administer privileged user accounts in accordance with a role-based access scheme
15. Monitor all privileged role assignments
16. Take defined actions once users no longer require privileged role assignments
17. Require that organization defined conditions be met to permit the use of shared or group accounts
18. Terminate or change shared or group account credentials when members leave the group
19. Monitor system accounts for atypical usage
20. Report any detection of atypical usage on system accounts to defined personnel or roles

8.3 ACCESS ENFORCEMENT

Approved authorizations for logical access to the system will be enforced in accordance with applicable PRC-Saltillo defined, identity-based, role-based, attribute-based policies.

8.4 INFORMATION FLOW ENFORCEMENT

To regulate where information can travel, PRC-Saltillo information systems enforce approved authorizations for controlling the flow of information within the system and between interconnected systems. Acceptable information flow is based on organization-defined information flow control policies.

PRC-Saltillo information systems separate the information flow logically or physically using defined mechanisms and/or techniques to accomplish defined separation by information type.

8.5 SEPARATION OF DUTIES

PRC-Saltillo maintains a "separation of duties" framework that has been documented and implemented across the organization to define the duties of individual employees, prevent malicious activity without collusion, and assign information system access authorizations.

8.6 LEAST PRIVILEGE

PRC-Saltillo follows the "least privilege" concept. Only the minimum necessary system preferences required to perform job duties are granted to an individual. The following measures have been put in place to ensure compliance with the least privilege requirements:

1. Explicit authorization must be granted through the account authorization process to receive authorized access to a service provider defined list of security functions and relevant security information.
2. Individuals with access to information system accounts, roles, or other security functions are required to use a unique, non-privileged account when performing non-administrative functions.
3. Privileged accounts on the information system are restricted to predefined personnel or roles.
4. Information systems regularly audit the execution of privileged functions.
5. Non-privileged users are prevented from executing privileged functions including disabling, circumventing, or altering implemented security safeguards or countermeasures.

8.7 UNSUCCESSFUL LOG IN ATTEMPTS

Users are limited to fifteen (15) consecutive invalid log-in attempts during a one (1) hour period. If the user exceeds the maximum number of unsuccessful log-in attempts, the account/node will be automatically locked for thirty (30) minutes.

8.8 REMOTE ACCESS SECURITY

PRC-Saltillo information systems can be accessed outside of the network by using the SonicWALL Global VPN Client.

Access to VPN can be obtained by:

1. Getting approval by and individuals manager or responsible party
2. Completing the Telecommunications Policy
3. Enrolling in MFA using the https://pass.prc-saltillo.com site.

MFA is a requirement for all external access to internal systems or systems setup/installed after Jan 2023 that contain PHI.

8.9 CONCURRENT SESSIONS

PRC-Saltillo limits the number of concurrent sessions for privileged users to two (2) sessions and two (2) sessions for non-privileged users on each system.

8.10 SESSION LOCK AND TERMINATION

PRC-Saltillo information systems have a session lock that is triggered after no more than thirty (30) minutes of inactivity or upon receiving a user request. The system will retain the session lock until the user re-established access using their PRC-Saltillo identification.

Upon activation of a session lockout, information previously visible on the display is concealed with a login screen. User sessions will be automatically terminated after 30 minutes.

8.11 ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

User actions that can be performed on information systems without identification or authentication are prohibited.

8.12 REMOTE ACCESS

Usage restrictions, configuration and connection requirements, and implementation guidance have been established and documented for each type of remote access allowed by PRC-Saltillo. All remote access to the information system is authorized prior to allowing such connections.

PRC-Saltillo uses Graylog to facilitate the monitoring of remote access methods, allowing event auditing across information system components. The confidentiality and integrity of all remote access sessions is protected using encryption and the information system is configured to route all remote accesses through a limited number of managed access control points (e.g., external firewall, load balancer, etc.).

Execution of privileged commands and access to security-relevant information via remote access are only authorized for compelling operational needs. Any unauthorized remote access connections to the system will be disconnected within fifteen (15) minutes of discovery.

8.13 WIRELESS ACCESS

To ensure secure wireless access and wireless operations, usage restrictions, configuration and connection requirements, and implementation guidance have been established for all wireless access.

All wireless access to information systems must be explicitly authorized prior to establishing connections and all wireless access to the system is protected using authentication and encryption, while ensuring authentication is applied to users, devices, or both as necessary.

8.14 ACCESS CONTROL FOR MOBILE DEVICES

PRC-Saltillo has not yet implemented usage restrictions and implementation guidance for organization-controlled mobile devices. All mobile device connections, given they meet established usage restrictions, are authorized.

8.15 USE OF EXTERNAL INFORMATION SYSTEMS AND INFORMATION SHARING

Where applicable, PRC-Saltillo has established terms and conditions allowing authorized access to PRC-Saltillo information systems from external information systems. Additional terms and conditions have been established allowing authorized individuals to process, store, and/or transmit PRC-Saltillo controlled information using the external information systems.

PRC-Saltillo permits authorized individuals to use an external information system to access PRC-Saltillo systems or to process, store, or transmit organization-controlled information only when the implementation of required security can be verified on the external system.

The use of PRC-Saltillo controlled portable storage devices by authorized individuals on external information systems is prohibited.

To facilitate information sharing, PRC-Saltillo has enabled authorized users with the ability to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for defined information sharing circumstances where user discretion is required. Additionally, PRC-Saltillo must employ defined automated mechanisms or manual processes to assist users in making information sharing/collaboration decisions.

8.16 PUBLICLY ACCESSIBLE CONTENT

Only designated and authorized individuals are permitted to post publicly accessible information onto the information system. Authorized individuals are trained to ensure that publicly accessible information does not contain non-public information.

prc-saltillo

END USER LICENSE AGREEMENT

This End User License Agreement (EULA) and all of the terms and conditions contained herein along with the PRC-Saltillo Privacy Policy (**prc-saltillo.com/privacy-policy**) and Terms of Use (**prc-saltillo.com/terms-of-use**) ("Agreement") constitute a legal agreement between the person, company or organization ("you" or "user") that has acquired PRC- Saltillo Software ("Software") and the Prentke Romich Company, doing business as PRC-Saltillo® ("PRC-Saltillo", "we," "us" or "our"). This Agreement governs your use of Demonstration Software acquired through download for use on your computer and Language Software loaded on to a PRC-Saltillo speech-generating device ("Device"). PRC-Saltillo Demonstration Software may include ChatEditor™, NuVoice® PASS™, and Empower® Demo Software. PRC-Saltillo Language Software is distributed on PRC-Saltillo speech-generating devices including those within the Accent®, NovaChat®, and Via® lines of devices.

By obtaining and using or downloading the Software, you agree to be bound by this Agreement and all its terms and conditions.

If you do not agree to the terms of this Agreement, you should not install or use the Software. If you have already installed it, you should immediately uninstall the Software as you shall have no right to use it. If you purchased the Software as part of a speech generating device, promptly contact PRC-Saltillo for instructions on return of the unused Device for a refund. **ANY USE OF THE SOFTWARE, INCLUDING BUT NOT LIMITED TO USE ON THE DEVICE, WILL CONSTITUTE YOUR AGREEMENT TO THIS EULA (OR RATIFICATION OF ANY PREVIOUS CONSENT).**

PRC-Saltillo and its suppliers own all of the intellectual property in the Software available on its Devices and for download on other Devices. This license grants you permission to use it only in accordance with the terms of this Agreement.

Grant of Software License

This EULA grants you a limited, terminable, non-exclusive license to use the Software for the purposes described in the documentation related to the Software. This also governs any Software upgrades provided by PRC-Saltillo that replace and/or supplement the original version of the Software downloaded, unless such upgrades are accompanied by a separate license, in which case the terms of that license will govern.

You may:

a) install PRC-Saltillo Demonstration Software on any Device that you own or control or use PRC-Saltillo Software on your PRC-Saltillo speech generating device

b) use the Software for personal, educational purposes only

c) make one copy of the Software for back-up, archival purposes, provided such copy contains all of the original proprietary notices provided with or otherwise relating to the Software

You may not use, or permit others to use, the Software except under the terms expressly listed in the Agreement. A separate license must be obtained or purchased for each end user. Without limiting the generality of the foregoing, you shall not, and shall not permit anyone else to:

a) use the Software on any Device that you do not own or control

b) use the Software for service bureau, time-sharing or other similar purposes

c) modify, translate, reverse engineer, decompile, attempt to derive the source code of, disassemble (except to the extent that this restriction is expressly prohibited by law), or create derivative works based upon the Software

d) copy the Software (except as permitted above), any updates or any part thereof

e) rent, lease, distribute, or otherwise transfer rights to the Software (unless so allowed elsewhere in this Agreement)

f) develop, sell, or distribute other software or applications that integrate with the Software or otherwise make use of the Data

g) remove any proprietary notices or labels on or relating to the Software; or

h) use the Software in any manner that could impair any website that we may own or operate currently or in the future, including but not limited to the PRC-Saltillo website located at prc-saltillo.com ("Website") or in any way or interfere with any party's use and enjoyment of the Website

Without limiting the foregoing, the Software and all information or data downloaded by or in connection with it are protected by the copyright law of the United States and international copyright treaties, as well as other proprietary rights.

Transfer of Software License

Software transfer allowed only in connection with Software transferred with a PRC-Saltillo Device. You may permanently transfer rights under this EULA only as part of a permanent sale or transfer of a Device, and only if the recipient agrees to this EULA. If the Software is an upgrade, any transfer must also include all prior versions of Software.

All right, title, and interest in and to the Software (including without limitation all intellectual property rights) shall remain with us.

Use of Information

To facilitate product support, product development and improvement as well as other services to you, you agree that PRC-Saltillo or other third parties authorized by PRC-Saltillo may use cookies, web beacons and other analytic technologies to collect, use, store and transmit non-personally identifiable technical and related information regarding your Device, including unique telemetry I.D., device make and model, and operating system. In addition, such parties may collect, store, use and transmit non-personally identifiable software usage metrics, statistics, or analytics.

Termination

You acknowledge that we have the right to restrict access to, terminate and/or otherwise modify the Software for any reason, including but not limited to a breach of any provision of the Terms of Use on our Website or this Agreement. On termination, you must destroy all copies of the Software and any information or data downloaded from the Software to your Device.

Additional Disclaimers of Warranties

PLEASE NOTE THE FOLLOWING IMPORTANT DISCLAIMERS OF WARRANTIES:

THE SOFTWARE IS PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED. WE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO WARRANTIES OF TITLE OR IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, COMPATABILITY, SECURITY, ACCURACY OR NON-INFRINGEMENT. THIS SOFTWARE DOES NOT INTENTIONALLY INFRINGE ON ANY THIRD-PARTY INTELLECTUAL PROPERTY RIGHTS AND PRC-SALTILLO DOES NOT WARRANT AGAINST NON-INFRINGEMENT.

NEITHER PRC-SALTILLO, ANY OF OUR AFFILIATES, NOR ANY OF OUR OR THEIR RESPECTIVE LICENSORS, LICENSEES, SERVICE PROVIDERS OR SUPPLIERS WARRANT THAT THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE OR THAT DEFECTS WILL BE CORRECTED.

YOUR DOWNLOAD AND USE OF THE SOFTWARE IS AT YOUR SOLE RISK AND YOU WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE TO YOUR COMPUTER SYSTEM OR DEVICE OR LOSS OF DATA THAT RESULTS FROM SUCH USE.

NEITHER PRC-SALTILLO, ANY OF OUR AFFILIATES, NOR ANY OF OUR OR THEIR RESPECTIVE LICENSORS, LICENSEES, SERVICE PROVIDERS OR SUPPLIERS WARRANT OR MAKE ANY REPRESENTATIONS REGARDING THE USE OR THE RESULTS OF THE USE OF THE SOFTWARE IN TERMS OF THEIR CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE.

SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF OR LIMITATIONS ON IMPLIED WARRANTIES OR THE LIMITATIONS ON THE APPLICABLE STATUTORY RIGHTS OF A CONSUMER, SO SOME OR ALL OF THE ABOVE EXCLUSIONS AND LIMITATIONS MAY NOT APPLY TO YOU.

Additional Limitation of Liability

YOU EXPRESSLY UNDERSTAND AND AGREE THAT WE AND OUR AFFILIATES, SUPPLIERS AND LICENSORS SHALL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, EXEMPLARY OR PUNITIVE DAMAGES, OR ANY OTHER DAMAGES WHATSOEVER, INCLUDING BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS, GOODWILL, USE, DATA OR OTHER INTANGIBLE LOSSES (EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES), ARISING OUT OF, OR RESULTING FROM, (A) THE USE OR THE INABILITY TO USE THE SOFTWARE; OR (B) THE COST OF PROCUREMENT OF SUBSTITUTE GOODS AND SERVICES RESULTING FROM USE OF THE SOFTWARE, OR ANY DEFECT THEREIN. IN NO EVENT SHALL OUR TOTAL LIABILITY TO YOU FOR ALL DAMAGES, LOSSES, AND CAUSES OF ACTION IN CONNECTION WITH THE SOFTWARE (WHETHER IN CONTRACT, TORT (INCLUDING, BUT NOT LIMITED TO, NEGLIGENCE), OR OTHERWISE) EXCEED THE AMOUNT PAID BY YOU, IF ANY, FOR THE SOFTWARE. IF YOU ARE DISSATISFIED WITH ANY PORTION OF THE SOFTWARE, OR WITH ANY PROVISION OF THIS AGREEMENT, YOUR SOLE AND EXCLUSIVE REMEDY IS THE DISCONTINUATION OF YOUR USE OF THE SOFTWARE.

Symbol Applications/Software

This EULA specifically covers PRC-Saltillo Software and future downloads of such Software. PRC-Saltillo Software contains symbols proprietary to PRC-Saltillo and symbols used under license from others. These symbols include Minspeak®, Pixon®, the Tobii Dynavox PCS® symbol library, the news2you SymbolStix® symbol library, and Metacom symbols. PRC-Saltillo owns or holds a license for all of the intellectual property in the Software. The use of any Software that contains or provides access to proprietary symbol sets or any part thereof, is governed by the following provisions in addition to the rest of the terms and conditions of this Agreement.

The symbols accessed through this Software may not be used to create materials in print or electronic form, whether for communication or instruction, except by a single user in conjunction with use of this Software. Distribution of any content or materials using symbols in other formats (e.g. .pdf or PDF, .ppt or PowerPoint, .doc or WORD, or similar software formats used to display and/or transmit text and/or images) is not permitted. Users of this Software may not rent, lease, or lend symbols, or provide them to any online service or commercial hosting services. Users may not sublicense, assign, or transfer any rights to the symbols, or authorize all or any portion of the symbols to which the user has access to be copied onto any computer or other device.

Minspeak® icons and Pixon® symbols are registered trademarks of PRC-Saltillo.

The Picture Communication Symbols ("PCS") accessed with PRC-Saltillo Software may not be used to create materials in print or electronic form, whether for communication or instruction, except by a single user in conjunction with use of this Device. PCS symbols may be distributed solely in Boardmaker file formats designated with a ".bm2", ".zip", or ".zbp" file extension. Distribution of any content or materials using PCS symbols in other formats (e.g. .pdf or PDF, .ppt or PowerPoint, .doc or WORD, or similar software formats used to display and/or transmit text and/or images) is not permitted.

SymbolStix symbols are used in PRC-Saltillo Software with permission under license from n2y, LLC. The Library of SymbolStix Character/Logo Symbols Contained in PRC-Saltillo software is included free of charge, may be used solely for communication purposes, and may not be sold, copied, or otherwise exploited for any type of profit. SymbolStix symbols may be distributed for personal use only when a SymbolStix Prime subscription is purchased.

Metacom is a trademark of Annette Kitzinger. The Metacom symbols are used with the kind permission of Annette Kitzinger. METACOM Symbole © Annette Kitzinger. Reproductions for the automated analysis of METACOM symbols for information retrieval (text and data mining) are not permitted and remain reserved to the copyright holder.

Product Specific Information

ChatEditor, NuVoice PASS, and Empower Demonstration Software

IMPORTANT – PRC-Saltillo Demonstration Software is not intended to be an emergency call device nor the sole means of communication for any individual.

NovaChat, Via, and Accent Device Language Software

Accent: You may use the Software only on your PRC-Saltillo Device.

USER, OR A PARTY WITH AUTHORITY TO BIND USER, UNDERSTANDS AND ACKNOWLEDGES THAT PRC-SALTILLO DOES NOT WARRANT ANY FUNCTIONALITY OF THIS SPEECH GENERATING DEVICE OUTSIDE THE TERMS OF ITS EXPRESS WARRANTY RELATING TO THE INTENDED USE OF SPEECH GENERATION. PRC-SALTILLO DOES NOT WARRANT ANY THIRD-PARTY SOFTWARE, NOR IS IT RESPONSIBLE FOR ANY INJURY, DAMAGE OR CLAIMS ARISING FROM THE FUNCTION OR MALFUNCTION OF ANY THIRD-PARTY TECHNOLOGY, WEBSITES, PRODUCTS, AND SOFTWARE. ADDITIONAL USES MAY REQUIRE FURTHER CLINICAL DETERMINATIONS BEYOND THE SCOPE OF AN EVALUATION FOR SPEECH GENERATION DEVICES.

Via Device Language Software

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, APPLE WILL HAVE NO WARRANTY OBLIGATION WHATSOEVER WITH RESPECT TO THE SOFTWARE, AND ANY CLAIMS, LOSSES, LIABILITIES, DAMAGES, COSTS OR EXPENSES ATTRIBUTABLE TO FAILURE TO CONFORM WITH A WARRANTY MADE UNDER THIS AGREEMENT (IF ANY), WILL BE PRC-SALTILLO'S SOLE RESPONSIBILITY.

Use of language software on the Via line of devices is also governed by the applicable license agreement for the particular iOS application.

- Find the LAMP Words for Life EULA here: **lampwflapp.com/eula**
- Find the TouchChat EULA here: **touchchatapp.com/eula**
- Find the Dialogue AAC EULA here: **prc-saltillo.com/dialogueEULA**
- Find the Eloquence EULA here: **prc-saltillo.com/eula-eloquence**

Accent Device Language Software

PRC-Saltillo Accent Devices include software licensed by PRC-Saltillo from Microsoft Licensing Inc. or its affiliates ("MS"). Those installed software products of MS origin, as well as associated media, printed materials and "online" or electronic documentation (software) are protected by international intellectual property laws and treaties.

IF YOU HAVE RECEIVED ANY WARRANTIES REGARDING THE DEVICE OR SOFTWARE, THOSE WARRANTIES DO NOT ORIGINATE FROM, AND ARE NOT BINDING ON, MS. THE SOFTWARE IS NOT FAULT TOLERANT. PRC-SALTILLO HAS INDEPENDENTLY DETERMINED HOW TO USE THE SOFTWARE AND MS HAS RELIED UPON PRC-SALTILLO TO CONDUCT SUFFICIENT TESTING TO DETERMINE THAT THE SOFTWARE IS SUITABLE FOR SUCH USE.

Note on Java Support. The Software may contain support for programs written in Java. Java technology is not fault tolerant and is not designed, manufactured, or intended for use or resale as online control equipment in hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or weapons systems, in which the failure of Java technology could lead directly to death, personal injury or severe physical or environmental damage. Sun Microsystems, Inc. has contractually obligated MS to make this disclaimer.

Export and Other Laws

You may not use the Software in contravention of any federal, state, or other applicable laws. Without limiting the foregoing, the Software may be subject to United States export control laws, and you agree to comply strictly with all such laws which are now or hereafter in effect. In particular, but without limitation, you may not export or re-export the Software: (a) into any United States embargoed countries or (b) to anyone on the United States Treasury Department's list of Specially Designated Nationals or the United Sates Department of Commerce Denied Person's List or Entity List. By using the Software, you represent and warrant that you are not located in any such country or on any such list. You also agree that you will not use these products for any purposes prohibited by United States law, including, without limitation, the development, design, manufacture, or production of missiles, nuclear or chemical or biological weapons.

Product Questions, Comments, and Claims

Submit all comments or questions about this license to our Feedback Portal at: https://www.prc-saltillo.com/feedback

Indemnification

You agree to indemnify, hold harmless and, at our option, defend us and our affiliates, and our and their officers, directors, employees, stockholders, agents and representatives from any and all third party claims, liability, damages and/or costs (including, but not limited to, reasonable attorney's fees and expenses) arising from your improper use of the software, your violation of this Agreement, or your infringement, or the infringement or use by any other user of your account, of any intellectual property or other right of any person or entity.

Translations, Governing Law, and Choice of Forum

PRC-Saltillo may translate this Agreement into various languages. However, the English language version is the original and controlling Agreement, and all other language versions are translations for information purposes only. In the event of any conflict or inconsistency between any terms of this Agreement in English and in any translation, the English language version of this Agreement shall prevail.

This Agreement shall be governed by and construed in accordance with the laws of the State of Ohio, without giving effect to any principles of conflicts of law. You agree that any action at law or in equity arising out of or relating to your use of this Software or this Agreement shall be filed only in the state or federal courts located in or having jurisdiction over Wayne County in the State of Ohio and you hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action.

Waiver of Breach

Our waiver of a breach of any provision of this Agreement by any user shall not operate or be construed as a waiver of any subsequent breach by you or any other user.