

**MASSACHUSETTS STUDENT DATA PRIVACY AGREEMENT  
VERSION (2018)**

**Westwood Public Schools**

**and**

**Bloomz, Inc.**

**May 20, 2019**

This Massachusetts Student Data Privacy Agreement (“DPA”) is entered into by and between the school district, Westwood Public Schools (hereinafter referred to as “LEA”) and Bloomz, Inc. (hereinafter referred to as “Provider”) on May 20, 2019. The Parties agree to the terms as stated herein.

## RECITALS

**WHEREAS**, the Provider has agreed or will agree to provide the Local Education Agency (“LEA”) with certain digital educational services (“Services”) as described in Article I and Exhibit “A”; and

**WHEREAS**, the Provider, by signing this Agreement, agrees to allow the LEA to offer school districts in Massachusetts the opportunity to accept and enjoy the benefits of the DPA for the Services described, without the need to negotiate terms in a separate DPA; and

**WHEREAS**, in order to provide the Services described in Article 1 and Appendix A, the Provider may receive or create and the LEA may provide documents or data that are covered by several federal statutes, among them, the Federal Educational Rights and Privacy Act (“FERPA”) at 20 U.S.C. 1232g and 34 CFR Part 99, Children’s Online Privacy Protection Act (“COPPA”), 15 U.S.C. 6501-6502; Protection of Pupil Rights Amendment (“PPRA”) 20 U.S.C. 1232h; the Individuals with Disabilities Education Act (“IDEA”), 20 U.S.C. §§ 1400 *et. seq.*; and

**WHEREAS**, the documents and data transferred from Massachusetts LEAs and created by the Provider’s Services are also subject to several Massachusetts student privacy laws, including Massachusetts student record regulations, 603 C.M.R. 23.00, Massachusetts General Law, Chapter 71, Sections 34D to 34H and 603 CMR 28.00; and

**WHEREAS**, the Parties wish to enter into this DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties.

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

## ARTICLE I: PURPOSE AND SCOPE

- 1. Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Student Data (as defined in Exhibit “C”) transmitted to Provider from the LEA pursuant to Exhibit “A”, including compliance with all applicable state privacy statutes, including the FERPA, PPRA, COPPA, IDEA, 603 C.M.R. 23.00, 603 CMR 28.00, and Massachusetts General Law, Chapter 71, Sections 34D to 34H. In performing these services, to the extent Personally Identifiable Information (as defined in Exhibit “C”) from Pupil Records (as defined in Exhibit “C”) are transmitted to Provider from LEA, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA. Control duties are set forth below.
- 2. Nature of Services Provided.** The Provider has agreed to provide the following digital educational services described in Exhibit “A”.

3. **Student Data to Be Provided.** In order to perform the Services described in this Article and Exhibit "A", LEA shall provide the categories of data described in the Schedule of Data, attached hereto as Exhibit "B".
4. **DPA Definitions.** The definition of terms used in this DPA is found in Exhibit "C". In the event of a conflict, definitions used in this DPA shall prevail over terms used in all other writings, including, but not limited to, a service agreement, privacy policies or any terms of service.

## **ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS**

1. **Student Data Property of LEA.** All Student Data or any other Pupil Records transmitted to the Provider pursuant to this Agreement is and will continue to be the property of and under the control of the LEA, or to the party who provided such data (such as the student or parent.). The Provider further acknowledges and agrees that all copies of such Student Data or any other Pupil Records transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are also subject to the provisions of this Agreement in the same manner as the original Student Data or Pupil Records. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data or any other Pupil Records contemplated per this Agreement shall remain the exclusive property of the LEA. For the purposes of FERPA and state law, the Provider shall be considered a School Official, under the control and direction of the LEAs as it pertains to the use of student data notwithstanding the above. The Provider will cooperate and provide Student Data within ten (10) days at the LEA's request. Provider may transfer pupil-generated content to a separate account, according to the procedures set forth below.
2. **Parent Access.** LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review personally identifiable information on the pupil's records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. Provider shall cooperate and respond within ten (10) days to the LEA's request for personally identifiable information in a pupil's records held by the Provider to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Provider to review any of the Pupil Records of Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.
3. **Separate Account.** Provider shall, at the request of the LEA, transfer Student Generated Content to a separate student account.
4. **Third Party Request.** Should a Third Party, including, but not limited to law enforcement, former employees of the LEA, current employees of the LEA, and government entities, contact Provider with a request for data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the data directly from the LEA and shall cooperate with the LEA to collect the required information. Provider shall notify the LEA in advance of a

compelled disclosure to a Third Party, unless legally prohibited. The Provider will not use, disclose, compile, transfer, sell the Student Data and/or any portion thereof to any third party or other entity or allow any other third party or other entity to use, disclose, compile, transfer or sell the Student Data and/or any portion thereof, without the express written consent of the LEA or without a court order or lawfully issued subpoena. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

5. **No Unauthorized Use.** Provider shall not use Student Data or information in a Pupil Record for any purpose other than as explicitly specified in this DPA.
6. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions pursuant to this DPA, whereby the Subprocessors agree to protect Student Data in manner consistent with the terms of this DPA.

#### ARTICLE III: DUTIES OF LEA

1. **Provide Data In Compliance With Laws.** LEA shall provide data for the purposes of the DPA in compliance with the FERPA, PPRA, IDEA, 603 C.M.R. 23.00, 603 CMR 28.00, and Massachusetts General Law, Chapter 71, Sections 34D to 34H, and the other privacy statutes quoted in this DPA. LEA shall ensure that its annual notice under FERPA includes vendors, such as the Provider, as "School Officials."
2. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted data.
3. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known or suspected unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

#### ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all Massachusetts and Federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, , 603 C.M.R. 23.00 and Massachusetts General Law, Chapter 71, Sections 34D to 34H.
2. **Authorized Use.** Student Data shared pursuant to this DPA, including persistent unique identifiers, shall be used for no purpose other than the Services stated in this DPA and as authorized under the statutes referred to in subsection (1), above. Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, any student data, meta data, user content or other non-public

information and/or personally identifiable information contained in the Student Data, without the express written consent of the LEA, unless it fits into the de-identified information exception in Article IV, Section 4, or there is a court order or lawfully issued subpoena for the information.

3. **Employee Obligation.** Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the data shared under this DPA. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the DPA.
  
4. **No Disclosure.** De-identified information, as defined in Exhibit "C", may be used by the Provider for the purposes of development, research, and improvement of educational sites, services, or applications, as any other member of the public or party would be able to use de-identified data pursuant to 34 CFR 99.31(b). The Provider and LEA agree that the Provider cannot successfully de-identify information if there are fewer than twenty (20) students in the samples of a particular field or category of information collected, *i.e.*, twenty students in a particular grade, twenty students of a particular race, or twenty students with a particular disability. Provider agrees not to attempt to re-identify de-identified Student Data and not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Provider shall not copy, reproduce or transmit any data obtained under this DPA and/or any portion thereof, except as necessary to fulfill the DPA.
  
5. **Disposition of Data.** Provider shall dispose or delete all personally identifiable data obtained under the DPA when it is no longer needed for the purpose for which it was obtained and transfer said data to LEA or LEA's designee within sixty (60) days of the date of termination and according to a schedule and procedure as the Parties may reasonably agree. Nothing in the DPA authorizes Provider to maintain personally identifiable data obtained under any other writing beyond the time period reasonably needed to complete the disposition. Disposition shall include (1) the shredding of any hard copies of any Pupil Records; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable. Provider shall provide written notification to LEA when the Data has been disposed. The duty to dispose of Student Data shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of the DPA. The LEA may employ a "Request for Return or Deletion of Student Data" FORM, A Copy of which is attached hereto as Exhibit "D"). Upon receipt of a request from the LEA, the Provider will immediately provide the LEA with any specified portion of the Student Data within three (3) calendar days of receipt of said request.
  
6. **Advertising Prohibition.** Provider is prohibited from using Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing or advertising efforts by a Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to Client; or (d) use the

Student Data for the development of commercial products or services, other than as necessary to provide the Service to Client.

## ARTICLE V: DATA PROVISIONS

1. **Data Security.** The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in Exhibit "F" hereto. These measures shall include, but are not limited to:
  - a. **Passwords and Employee Access.** Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data to employees or contractors that are performing the Services. Employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Records shall pass criminal background checks.
  - b. **Destruction of Data.** Provider shall destroy or delete all Personally Identifiable Data contained in Student Data and obtained under the DPA when it is no longer needed for the purpose for which it was obtained or transfer said data to LEA or LEA's designee, according to a schedule and procedure as the parties may reasonable agree. Nothing in the DPA authorizes Provider to maintain personally identifiable data beyond the time period reasonably needed to complete the disposition.
  - c. **Security Protocols.** Both parties agree to maintain security protocols that meet industry best practices in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all data obtained or generated pursuant to the DPA in a secure computer environment and not copy, reproduce, or transmit data obtained pursuant to the DPA, except as necessary to fulfill the purpose of data requests by LEA. The foregoing does not limit the ability of the Provider to allow any necessary service providers to view or access data as set forth in Article IV, section 4.
  - d. **Employee Training.** The Provider shall provide periodic security training to those of its employees who operate or have access to the system. Further, Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.
  - e. **Security Technology.** When the service is accessed using a supported web browser, Secure Socket Layer ("SSL"), or equivalent technology shall be employed to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Provider shall host data pursuant to the DPA in an environment using a firewall that is periodically updated according to industry standards.
  - f. **Security Coordinator.** Provider shall provide the name and contact information of Provider's Security Coordinator for the Student Data received pursuant to the DPA.
  - g. **Subprocessors Bound.** Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student Data in a manner consistent with the

terms of this Article V. Provider shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article.

- h. Periodic Risk Assessment.** Provider further acknowledges and agrees to conduct periodic risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.
  - i. Backups.** Provider agrees to maintain backup copies, backed up at least daily, of Student Data in case of Provider's system failure or any other unforeseen event resulting in loss of Student Data or any portion thereof.
  - j. Audits.** Upon receipt of a request from the LEA, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of the Student Record or any portion thereof. The Provider will cooperate fully with the LEA and any local, state, or federal agency with oversight authority/jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide full access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the Provider. Failure to cooperate shall be deemed a material breach of the Agreement.
- 2. Data Breach.** In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA within ten (10) days of the incident. Provider shall follow the following process:
- a.** The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.
  - b.** The security breach notification described above in section 2(a) shall include, at a minimum, the following information:

    - i.** The name and contact information of the reporting LEA subject to this section.
    - ii.** A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
    - iii.** If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
    - iv.** Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
    - v.** A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

- c. At LEA's discretion, the security breach notification may also include any of the following:
  - i. Information about what the agency has done to protect individuals whose information has been breached.
  - ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.
- d. Provider agrees to adhere to all requirements in the Massachusetts Data Breach law and in federal law with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
- e. Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a copy of said written incident response plan.
- f. At the request and with the assistance of the District, Provider shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above.

#### ARTICLE VI: MISCELLANEOUS

1. **Term.** The Provider shall be bound by this DPA for so long as the Provider maintains any Student Data. Notwithstanding the foregoing, Provider agrees to be bound by the terms and obligations of this DPA for three (3) years.
2. **Termination.** In the event that either party seeks to terminate this DPA, they may do so by mutual written consent and as long as any service agreement or terms of service, to the extent one exists, has lapsed or has been terminated.  
 The LEA may terminate this DPA and any service agreement or contract with the Provider if the Provider breaches any terms of this DPA.
3. **Effect of Termination Survival.** If the DPA is terminated, the Provider shall destroy all of LEA's data pursuant to Article V, section 1(b).
4. **Priority of Agreements.** This DPA shall govern the treatment of student records in order to comply with the privacy protections, including those found in FERPA, IDEA, COPPA, PPR, 603 CMR 28.00, 603 C.M.R. 23.00, and Massachusetts General Law, Chapter 71, Sections 34D to 34H. In the event there is conflict between the terms of the DPA and any other writing, such as service agreement or with any other bid/RFP, terms of service, privacy policy, license agreement, or writing, the terms of this DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of any other agreement shall remain in effect.



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

The designated representative for the Provider for this Agreement is:

Name	Shannon Forte
Title	Sales Leader
Address	8335 165 <sup>th</sup> Ave NE, Redmond WA 98052
Telephone Number	954-296-6975
Email	Shannonf@bloomz.com

The designated representative for the LEA for this Agreement is:

Name	Steve Ouellette
Title	Technology Director
Address	220 Nahatan St., Westwood, MA 02090
Telephone Number	781-326-7500 x3364
Email	souellette@westwood.k12.ma.us

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

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

8. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND

CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF MASSACHUSETTS, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS OF NORFOLK COUNTY FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

9. **Authority.** Provider represents that it is authorized to bind to the terms of this Agreement, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the Student Data and portion thereof stored, maintained or used in any way.
10. **Waiver.** No delay or omission of the LEA to exercise any right hereunder shall be construed as a waiver of any such right and the LEA reserves the right to exercise any such right from time to time, as often as may be deemed expedient.
11. **Electronic Signature:** The parties understand and agree that they have the right to execute this Agreement through paper or through electronic signature technology, which is in compliance with Massachusetts and Federal law governing electronic signatures. The parties agree that to the extent they sign electronically, their electronic signature is the legally binding equivalent to their handwritten signature. Whenever they execute an electronic signature, it has the same validity and meaning as their handwritten signature. They will not, at any time in the future, repudiate the meaning of my electronic signature or claim that their electronic signature is not legally binding. They agree not to object to the admissibility of this Agreement as an electronic record, or a paper copy of an electronic document, or a paper copy of a document bearing an electronic signature, on the grounds that it is an electronic record or electronic signature or that it is not in its original form or is not an original.

Each party will immediately request that their electronic signature be revoked in writing if they discover or suspect that it has been or is in danger of being lost, disclosed, compromised or subjected to unauthorized use in any way. They understand that they may also request revocation at any time of their electronic signature for any other reason in writing.

If either party would like a paper copy of this Agreement, they may request a copy from the other party.

12. **Multiple Counterparts:** This Agreement may be executed in any number of identical counterparts. If so executed, each of such counterparts shall constitute this Agreement. In proving this Agreement, it shall not be necessary to produce or account for more than one such counterpart. Execution and delivery of this Agreement by .pdf or other electronic format shall constitute valid execution and delivery and shall be effective for all purposes (it being agreed that PDF email shall have the same force and effect as an original signature for all purposes).

**ARTICLE VII- GENERAL OFFER OF TERMS**

Provider may, by signing the attached Form of General Offer of Privacy Terms (General Offer, attached hereto as Exhibit "E"), be bound by the terms of this to any other school district who signs the acceptance in said Exhibit.

*[Signature Page Follows]*

IN WITNESS WHEREOF, the parties have executed this Massachusetts Student Data Privacy Agreement as of the last day noted below.

WESTWOOD PUBLIC SCHOOLS

Steve Ouellette Date: 5/28/19

Printed Name: Steve Ouellette Title: Director of Technology

BLOOMZ, INC.

Shannon Forte Date: May 16, 2019

Printed Name: Shannon Forte Title: Sales Leader

**EXHIBIT "A"**  
DESCRIPTION OF SERVICES

**Bloomz**, a web-based tool designed to help teachers and parents share information and photos through real-time communication and coordination.

**EXHIBIT "B"**  
**SCHEDULE OF DATA**

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	X
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	X
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	X
	Student class attendance data	X
Communications	Online communications that are captured (emails, blog entries)	X
Conduct	Conduct or behavioral data	X
Demographics	Date of Birth	opt in
	Place of Birth	
	Gender	opt in
	Ethnicity or race	
	Language information (native, preferred or primary language spoken by student)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	X
	Student grade level	X
	Homeroom	X
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email	X
	Phone	X
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	X
Schedule	Student scheduled courses	X
	Teacher names	X

Category of Data	Elements	Check if used by your system
Special Indicator	English language learner information	
	Low income status	
	Medical alerts	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
Special Indicator	Other indicator information-Please specify: <u>Pref Lang</u>	X
Category of Data	Elements	Check if used by your system
Student Contact Information	Address	
	Email	X
	Phone	X
Student Identifiers	Local (School district) ID number	
	State ID number	
	Vendor/App assigned student ID number	
	Student app username	
	Student app passwords	
Student Name	First and/or Last	
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	X
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures etc. Other student work data - Please specify:	
Transcript	Student course grades	
	Student course data	
	Student course grades/performance scores	

Category of Data	Elements	Check if used by your system
	Other transcript data -Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	

Category of Data	Elements	Check if used by your system
	Other transportation data - Please specify:	
Other	Please list each additional data element used, stored or collected by your application	

**EXHIBIT "C"**

**DEFINITIONS**

**De-Identifiable Information (DII):** De-Identification refers to the process by which the Vendor removes or obscures any Personally Identifiable Information ("PII") from student records in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them. The Provider's specific steps to de-identify the data will depend on the circumstances, but should be appropriate to protect students. Some potential disclosure limitation methods are blurring, masking, and perturbation. De-identification should ensure that any information when put together cannot indirectly identify the student, not only from the viewpoint of the public, but also from the vantage of those who are familiar with the individual. Information cannot be de-identified if there are fewer than twenty (20) students in the samples of a particular field or category, i.e., twenty students in a particular grade or less than twenty students with a particular disability.

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

**Personally Identifiable Information (PII):** The terms "Personally Identifiable Information" or "PII" shall include, but are not limited to, student data, metadata, and user or pupil-generated content obtained by reason of the use of Provider's software, website, service, or app, including mobile apps, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians. PII includes, without limitation, at least the following:

First Name	Home Address
Last Name	Subject
Telephone Number	Email Address
Discipline Records	Test Results
Special Education Data	Juvenile Dependency Records
Grades	Evaluations
Criminal Records	Medical Records
Health Records	Social Security Number
Biometric Information	Disabilities
Socioeconomic Information	Food Purchases
Political Affiliations	Religious Information
Text Messages	Documents
Student Identifiers	Search Activity
Photos	Voice Recordings
Videos	Date of Birth
Grade	Classes

**General Categories:**

**Indirect Identifiers:** Any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty

Information in the Student's Educational Record

Information in the Student's Email



**Provider:** For purposes of the DPA, the term “Provider” means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records.

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

**Pupil Records:** Means both of the following: (1) Any information that directly relates to a pupil that is maintained by LEA and (2) any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other local educational LEA employee.

**School Official:** For the purposes of this Agreement and pursuant to 34 CFR 99.31 (B), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of education records; and (3) Is subject to 34 CFR 99.33(a) governing the use and re-disclosure of personally identifiable information from student records. The definition of “school official” encompasses the definition of “authorized school personnel” under 603 CMR 23.02.

**Student Data:** Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students’ parents/guardians, that is descriptive of the student including, but not limited to, information in the student’s educational record or email, first and last name, home address, telephone number, email address, or other information allowing online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information text messages, documents, student identifies, search activity, photos, voice recordings or geolocation information. Student Data shall constitute Pupil Records for the purposes of this Agreement, and for the purposes of Massachusetts and Federal laws and regulations. Student Data as specified in Exhibit B is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student’s use of Provider’s services.

**Subscribing LEA:** An LEA that was not party to the original Services Agreement and who accepts the Provider’s General Offer of Privacy Terms.

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

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

**Third Party:** The term “Third Party” means an entity that is not the provider or LEA.

**EXHIBIT "D"**

**DIRECTIVE FOR DISPOSITION OF DATA**

[Name or District or LEA] directs [Name of Company] to dispose of data obtained by Company pursuant to the terms of the DPA between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

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

[Insert categories of data here]

\_\_\_ Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

\_\_\_ Disposition shall be by destruction or deletion of data.

\_\_\_ Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

[Insert or attach special instructions.]

3. Timing of Disposition

Data shall be disposed of by the following date:

\_\_\_ As soon as commercially practicable

\_\_\_ By (Insert Date)

4. Signature

\_\_\_\_\_  
(Authorized Representative of LEA)

\_\_\_\_\_  
Date

5. Verification of Disposition of Data

\_\_\_\_\_  
Authorized Representative of Company

\_\_\_\_\_  
Date

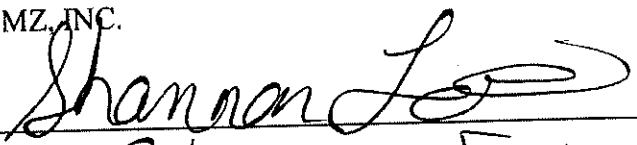
**EXHIBIT "E"**

**GENERAL OFFER OF PRIVACY TERMS**

**1. Offer of Terms**

Provider offers the same privacy protections found in this DPA between it and the LEA to any other school district ("Subscribing LEA") who accepts this General Offer through its signature below. The Provider agrees that the information on the next page will be replaced throughout the Agreement with the information specific to the Subscribing LEA filled on the next page for the Subscribing LEA. This General Offer shall extend only to privacy protections and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provide by LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statutes; (2) a material change in the services and products subject listed in the Originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Provider shall notify the LEA in the event of any withdrawal so that this information may be transmitted to the Subscribing LEAs.

BLOOMZ, INC.

BY:  Date: May 16, 2019  
Printed Name: Shannon Forte Title/Position: Sales Leader

**2. Subscribing LEA**

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA's individual information is contained below. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA.

BY: \_\_\_\_\_ Date: \_\_\_\_\_  
Printed Name: \_\_\_\_\_ Title/Position: \_\_\_\_\_

SCHOOL DISTRICT NAME: \_\_\_\_\_

DESIGNATED REPRESENTATIVE OF LEA:

Name \_\_\_\_\_  
Title \_\_\_\_\_  
Address \_\_\_\_\_  
Telephone Number \_\_\_\_\_  
Email \_\_\_\_\_

COUNTY OF LEA: \_\_\_\_\_

**OPTIONAL: EXHIBIT "F"**  
**DATA SECURITY REQUIREMENTS**

Having robust data security policies and controls in place are the best ways to ensure data privacy. Please answer the following questions regarding the security measures in place in your organization:

1. Does your organization have a data security policy?  Yes  No

If yes, please provide it. See attached Bloomz Privacy Policy

2. Has your organization adopted a cybersecurity framework to minimize the risk of a data breach? If so which one(s):

ISO 27001/27002

CIS Critical Security Controls

NIST Framework for Improving Critical Infrastructure Security

Other: See attached Azure Hosting practices of Id Mngt, Access Control, and Security Groups. This allows the data to be accessible only to authenticated and authorized clients in a secure way. Azure handles updates and patches.

3. Does your organization store any customer data outside the United States?  Yes  No

4. Does your organization encrypt customer data both in transit and at rest?  Yes  No  
In Transit / at Rest

5. Please provide the name and contact info of your Chief Information Security Officer (CISO) or the person responsible for data security should we have follow-up questions.

Name: Nitin Bhandari

Contact information: nitin@bloomz.com

6. Please provide any additional information that you desire.

- [Bloomz](#)
- [Teachers](#)
- [Parents](#)
- [Schools](#)
- [Childcare](#)
- [PTA](#)
- [FAQ](#)
- [Blog](#)
- [Sign In](#)

## Bloomz Privacy Policy

Last Updated: August 23, 2016

At Bloomz, we take your privacy very seriously and we have taken every measure so you rest assured your information and your experience at Bloomz stays safe and private. This is why we have updated our Privacy Policy to reflect our commitment with your privacy as well as with common regulation in this matter, like the Children's Online Privacy Protection Act (COPPA), the Family Educational Rights and Privacy Act (FERPA, referred to in our Terms of Service) as well as the Student Privacy Pledge.

Our latest updates to our Privacy Policy below, also include a small summary to the right of the text, so you can easily browse and learn about our commitment to your privacy and security.



Bloomz is a proud signatory of the Student Privacy Pledge.

Quick reference:

- [Information collected](#)
- [Authorized third parties](#)
- [Use of information](#)
- [Disclosure of information](#)
- [Underage usage, children's privacy and COPPA](#)
- [Our commitment to data security](#)
- [Updates to our privacy policy](#)
- [Questions and suggestions](#)

## Information Collected

Like many other services on the internet, Bloomz needs to collect some information from our users and their usage, to be able to provide you with the high quality experience you expect from us - rest assured, we

## What it means

We need some information to provide you with the best experience possible, and we will make every reasonable

will make every reasonable effort to insure that our service is secure and private in accordance with our promise of service and our policies . The information we collect (whether through our own means or through third parties, as explained below) can be in the form of:

- 1) Personal information you submit while creating an account with Bloomz or while using our service;
- 2) Automatically collected information; and,
- 3) Information from other sources.

effort to keep that information private and secure. There are three types of information we collect: Personal information you submit; automatically collected information; and, information from other sources.

### **Personal Information**

We collect personal information when you register through any of our platforms: website, mobile, or tablet applications (collectively, our "Apps"). Personal information is any information about you that is personally identifiable, such as your name, address, email address or phone number, third-party sign-in information (e.g. Facebook Connect, if applicable), and any other information that is not otherwise publicly available. In addition, if you send email invitations to friends or family to join your Bloomz network, those email addresses are, in some instances, also collected. In addition, there is other information that is stored in our service when either parents or teachers use our apps, including but not limited to: School and class information, including name and address, the student(s) name(s) or age, as well as the information sent over the service, including messages, announcements, images, events and other.

We collect the information you submit while registering for a Bloomz account or through its use, including your school information, posts and messages sent through Bloomz.

### **Automatically Collected Information**

When you use any of our services and apps (web, mobile or other, including when you open our email notifications) we, or our authorized third party service providers (explained below), may also collect information relating to your devices, including your device model, operating system, browser type, unique device identifier, IP address, mobile phone number, mobile network carrier, location, and event information (such as application installations). We may also automatically record certain information from your web browser by using different types of technology, including "clear gifs" or "web beacons." This "automatically collected" information may include your IP address or other device address or ID, web browser and/or device type, the web pages or sites that you visit just before or just after the Service, the pages you view on the Service, and the dates and times that you visit, access, or use the Service. This information is gathered for all users.

We collect information using our own or third party technology (including cookies) to provide you with the best experience possible.

### **Information from Other Sources:**

We may also obtain information, including personally identifiable information, from third parties and sources other than the Service, such as our partners or other service providers, according to their own policies and terms of use. We may also, at your direction, receive information from third party services that provide a mechanism to expose information you have provided to such third parties through the

We may use other sources (third party) to complement the information you provide and better serve your needs.

use of an application program interface (API), such as Facebook Connect or the Twitter API. If we combine or associate information from other sources with personally identifiable information that we collect through the Service, we will treat the combined information as personally identifiable information in accordance with this Privacy Policy.

### **Cookies and Similar Technologies**

We use cookies (pixel tags, and/or other similar technologies) to collect visitor information. Cookies are alphanumeric identifiers that we send to your computer's hard drive through your web browser. We may use both session cookies and persistent cookies. A session cookie disappears after you close your browser. A persistent cookie remains after you close your browser and may be used by your browser on subsequent visits. Like many services, we use these technologies to tailor the Service for you, and to help the Service work better for you - for example, for authentication, security and site integrity, localization, performance analytics, and other features and services. It is possible to delete cookies or prevent cookies from being used in your browser by turning the feature off. If you do so, you may not be able to use features of our service to their full.

We offer a range of features that use technologies like cookies, pixel tags ("pixels"), device or other identifiers and local storage to provide a seamless and safe experience.

## **Authorized Third Parties**

Providing a great experience is our outmost priority, but sometimes doing it all on our own is really hard, so we work with third party vendors, service providers, and other partners to help us provide the Service by performing tasks on our behalf. We may need to share or provide information (including personal information) to them to help them perform these business functions, for example sending emails on our behalf, database management services, database hosting, providing customer support software, and security. These service providers do not have the right to use your personal information we share with them beyond what is necessary to assist us. Additionally, these service providers must adhere to confidentiality and security obligations in a way that is consistent with this Privacy Policy.

Sometimes we just need a little help from our friends (and partners). But rest assured we are only sharing information needed to provide our service, and our partners will not use data for any other purpose. Even when we talk to you outside of our service, we don't share any personally identifiable information.

We may use third-party service providers to serve ads on our behalf across the Internet and on our Apps. They may collect anonymous information about your visits to our Apps and your interaction with our services. They may also use information about your visits to our Apps and other sites and mobile applications to target ads for products and services. For instance, they may collect web log data from you (such as IP address and information about your browser or operating system) or place or recognize a unique cookie on your browser to enable you to receive customized ads. Through this process, demographic or other interest data may be associated with your browser or device **in a non-personally identifiable manner**. No personally identifiable information is collected in this process. They do not know the name, address, email

address, phone number or any personally identifiable information about the user.

We also work with third party service providers to monitor certain pages of our Apps for such purposes as reporting traffic and other advertising statistics. Where authorized by us, these third party providers may use cookies and/or other monitoring technologies to compile anonymous statistics about our visitors. No personally identifiable information is transferred to these third party service providers. This information is collected directly by the third party, and Bloomz does not participate in that data transmission. Information collected by third parties in this manner is subject to that third party's own data collection, use, and disclosure policies.

## Use of Information

We use your information for the following general purposes: to operate, maintain, and improve our services, to contact you, for internal business purposes, and to customize any advertising and content you see in our apps. We use third party information you provide to us solely to provide services you specifically request.

We will also use all of the information that you provide and that we collect to understand and analyze the usages trends and preferences of our users, to improve our product, and to create new features and functionality. We may use your information to personalize our services, such as remembering your information so that you will not have to re-enter it during your visit or the next time you visit the Apps; provide customized advertisements and offer you other relevant products, content, and information; monitor and analyze the effectiveness of our services and third party marketing activities; monitor aggregate site usage metrics such as total number of visitors and pages viewed; and track your entries, submissions, and status in any promotions or other activities.

We will never use students' personally identifiable information, or collect, use, or share such information for any purposes beyond the authorized educational or school purposes, or as explicitly authorized by the student or parent. We will never target advertisements to students or sell students' personally identifiable information to third parties for any purpose.

When you invite recipients to join our service, we may contact them regarding our product and Service, using the appropriate form of communication. If they would prefer not to receive our communications, they may opt-out using the "Unsubscribe" or "STOP" instructions contained in those communications. Rest assured that we will not use the email addresses that you enter through email invitations, or your address books through any of our Apps to send marketing communications to your friends and family, unless they sign up for an account on their own and accept our terms and services.

The information we collect serves to run our business and to better tailor the experience for you. Emails of parents invited to join a classroom in Bloomz are automatically opted-in to classroom communications, so parents don't miss on important updates. Any person can opt-out of Bloomz communications following instructions included in those, or adjusting your notification preferences in the apps. Bloomz does NOT serve ads to students or use students personally identifiable information for any other purpose.



When a teacher invites parents to join their classroom on Bloomz via our SmartInvite feature in our app, the emails entered in the invitation will automatically be opted-in to classroom communications via email. We do this to ensure parents who don't know how to create an account don't miss on important updates from the teacher. Recipients can always opt-out by using the "Unsubscribe" instructions in those communications.

Your accounts also contain a calendar where you can store events and other key dates and details about friends and family. We may send you email reminders of the personalized dates you have entered in this calendar. You may decline to share certain personally identifiable information with us, in which case we may not be able to provide to you some of the features and functionality of the Service. You may update or correct your profile information and preferences at any time by accessing your account preferences page through the Service. Please note that while your changes are reflected promptly in active user databases, we may retain all information you submit for a variety of purposes, including backups and archiving, prevention of fraud and abuse, and analytics.

### **Disclosure of Information**

We do not sell or disclose your personally identifiable information to nonaffiliated parties except in connection with our services and the operation of our business as explained in this policy and our terms of service. We may disclose your personal information in the following ways:

We do not sell your personal information to third parties, and will not share information other than as established in this policy.

- Any information that you voluntarily choose to include in a publicly accessible area of the Apps, such as a public profile page, will be available to anyone who has access to that content, including other users.
- We provide personal information to nonaffiliated companies that we engage as contractors or agents to perform services for us, such as administering our websites, systems and software, hosting maintenance, and other such services. These third party service providers may have access to or process your information to the extent it is necessary for them to complete their contractual obligations to us. Generally, these disclosures are made under terms comparable to this policy, and the recipients are limited to using the information the purpose for which it was provided.
- We may disclose all the information we collect as described above to other companies to: comply with various reporting obligations; for business or marketing purposes; or to assist such parties in understanding our users' interests, habits, and usage patterns for certain programs, content, services, advertisements, promotions, and/or functionality available through the Apps.
- In response to subpoenas, court orders, or legal process, from law enforcement agencies or state and federal regulators, or as otherwise required by law;
- To assert or defend our legal rights, including fraud prevention;

- To protect the rights, property, or safety of other persons;
- As we deem appropriate to attempt to prevent physical or emotional harm to other persons and/or to their property based on overt or implied threat;
- In connection with an actual or proposed corporate merger, acquisition, asset purchase, or other transaction or proceeding involving all or part of the business or assets to which the information pertains.

## Children's Privacy

Our Apps are not intended for use by children under the age of 13. In fact, they are intended for teacher-parent communication. As part of that process, a teacher may request an individual student to input content that was created by that student, however, in no circumstance does that input become part of the student's profile without teacher approval. We will not knowingly collect personally identifiable information via this site from visitors under the age of 13, other than as previously stated. If we learn that personally identifiable information has been collected on the Service from persons under the age of 13 and without verifiable parental or teacher consent, then we will take the appropriate steps to delete this information.

We don't collect information from children under 13, thus Bloomz is COPPA compliant.

## COPPA Compliance

The COPPA Rule was put in place to protect kids' personal information on websites and online services — including apps — that are directed to children under 13. The Rule also applies to a general audience site that knows it's collecting personal information from kids that age. Because Bloomz doesn't collect information from children under 13, other than as previously stated, and any information related to students in Bloomz is knowingly entered by parents or by teachers with permission of the parents, Bloomz is COPPA compliant.

If you are a parent or guardian and discover that your child under the age of 13 has obtained an account on the Service, please alert us immediately at [support@bloomz.com](mailto:support@bloomz.com).

## Our Commitment to Data Security:

We use certain physical, managerial, and technical safeguards that are designed to improve the integrity and security of your information. As is the case with other online services, however, we cannot ensure or warrant the security of any information you transmit to us or store on

We take serious efforts to protect your information and the data in our service. As with any other online service, it is important you take

the Apps and you do so at your own risk. We also cannot guarantee that such information may not be accessed, disclosed, altered, or destroyed by breach of any of our physical, technical, or managerial safeguards. If we learn of a security systems breach, then we may attempt to notify you electronically so that you can take appropriate protective steps. We may post a notice through the Apps if a security breach occurs.

personal measures to protect your information (like safeguarding your password).

Similarly, although we may allow you to adjust your privacy settings to limit access to your information, please be aware that no security measures are perfect or impenetrable. We cannot control the actions of other users with whom you may choose to share your information. Therefore, we cannot and do not guarantee that information you post on the Apps will not be viewed by unauthorized persons. We are not responsible for circumvention of any privacy settings or security measures contained on the Website. You understand and acknowledge that, even after removal, copies of information that you have posted may remain viewable in cached and archived pages or if other users have copied or stored such information.

## Updates to Privacy Policy

We may modify this Privacy Policy from time to time by posting updates on this page. Please check back periodically to view any updates. In the event that the modifications materially alter your rights or obligations hereunder, we will make reasonable efforts to notify you of the change via email, if we have one on file, or generate a pop-up or similar notification when you access the Apps for the first time after such material changes are made. Our amended Privacy Policy will automatically take effect 30 days after it is made available through the Apps. If you do not agree with any changes to the Privacy Policy, you may terminate your account and stop using the Apps. Your continued use of the Apps after the revised Privacy Policy has become effective indicates that you have read, understood and agreed to the current version of the Privacy Policy.

We will always let you know by email and/or through our apps when we make significant changes to our Privacy Policy

## Questions and Suggestions

If you have questions about this Privacy Policy, you can contact us at [support@bloomz.com](mailto:support@bloomz.com) or through the feedback link on our Apps.

Email us at [support@bloomz.com](mailto:support@bloomz.com)

- Bloomz © 2016
- [About Us](#)
- [Jobs](#)
- [Privacy](#)
- [Terms](#)
- [Support](#)

# Risk Assessment Checklist to Help Prepare for NIST Cybersecurity Framework Implementation



## Disclaimer

*This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.*

*This document is provided "as-is." Information and views expressed in this document, including URL and other Internet website references, may change without notice. Customers reading this document bear the risk of using it.*

*This document does not provide customers with any legal rights to any intellectual property in any Microsoft product. Customers may copy and use this document for their internal reference purposes.*

*The information contained in this document must not be construed as legal advice. Customers must seek their own legal counsel for advice on compliance with regulatory requirements impacting their organization*

*Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.*

*NOTE: Certain recommendations in this document may result in increased data, network, or compute resource usage, and may increase a customer's license or subscription costs.*

*Version 1.1*

*© 2017 Microsoft. All rights reserved.*

## Introduction

On May 11, 2017, the President released Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. This Executive Order calls for organizations to provide a risk management report, to utilize shared IT services, and develop an action plan to implement the [NIST Cybersecurity Framework \(CSF\)](#).

The NIST CSF has four implementation Tiers that describe how an organization views and addresses cybersecurity risk and risk management processes: Partial (Tier 1), Risk Informed (Tier 2), Repeatable (Tier 3), and Adaptive (Tier 4). External guidance from Federal government departments and agencies, Information Sharing and Analysis Centers (ISACs), and other sources can be leveraged to assist in determining your organization's current and desired implementation Tier with respect to the Framework outcomes. This risk assessment checklist can be used to help your organization establish a high-level understanding of your security practices and identify areas of potential cybersecurity risk. By understanding the areas that have a higher risk, your organization can develop a plan to implement the full scope of outcomes described in the NIST CSF. Additional testing and evaluation should be conducted to determine the ability of your organization to align risk management practices with the NIST CSF as well as to determine a plan to implement requirements that are less than fully satisfied by current organization processes and procedures.

This checklist presents a series of broad questions that cover each of the Functions (Identify, Protect, Detect, Respond, and Recover) in the "Framework for Improving Critical Infrastructure Cybersecurity." In addition to the questions themselves, guidance has been provided on how to interpret responses. When addressing the questions below to gauge your organization's risk posture, responses may be assigned a designation of satisfactory, medium risk, or high risk. The "Response Assessment" section at the end of this document describes how to use the response assignments to assemble an overall picture of your organization's risk posture as it relates to the NIST CSF outcomes. Based on your responses, your organization can determine the areas in which your cybersecurity processes need improvement. These areas will need to be included in your action plan for implementing the NIST CSF outcomes at one of the implementation Tiers mentioned above.

The Service Trust Portal contains NIST CSF enablement whitepapers which demonstrate how your organization can use Microsoft Azure services to achieve the cybersecurity outcomes described in the NIST CSF Functions. For additional resources regarding customer responsibilities related to NIST CSF and the Cybersecurity Executive Order, or to provide feedback, please e-mail

[CyberEODHelp@microsoft.com](mailto:CyberEODHelp@microsoft.com).

**Risk Assessment Questionnaire:**

**What is your organization's IT security policy?**

Function	Category	Questions to gauge risk posture	Satisfactory Response (Score of 1)	Medium Risk Response (Score of 2)	High Risk Response (Score of 3)	Score
Identify Protect	Governance Asset Management	<ol style="list-style-type: none"> <li>1. Do you have a policy in place to manage and monitor your organization's security posture? (ID.GV-1)</li> <li>a. Do you have clearly defined information security roles and responsibilities? (ID.AM-6)</li> <li>b. Are your security roles coordinated and aligned with internal roles and external partners? (ID.GV-2)</li> <li>c. Do you have an awareness of the legal and regulatory security requirements in place for your organization? (ID.GV-3)</li> </ol>	A rigorous policy document with clearly defined procedures and roles exists, and there is organization-wide enforcement. Security is incorporated into day to day activities.	There are some ambiguous procedures and enforcement is not prioritized. Some individuals within the organization may have defined roles and responsibilities but there is not an organization-wide focus on security.	No policy document exists and there is no organization-wide enforcement. Users are not aware of security requirements or how to incorporate security into daily tasks.	
	Business Environment Data Security Protective Technology	<ol style="list-style-type: none"> <li>2. Do you perform business impact analysis for your organization's services and the infrastructure hosting those services? (ID.BE)                             <ol style="list-style-type: none"> <li>a. Have you identified and communicated your organization's role in the supply chain? (ID.BE-1)</li> <li>b. What is your organization's place in the critical infrastructure and your overall industry? (ID.BE-2)</li> <li>c. Have you established priorities for your organization's mission, objectives and activities and are they clearly communicated to all stakeholders? (ID.BE-3)</li> <li>d. Have you performed an analysis identifying critical functions and dependencies for the services that your organization provides? (ID.BE-4)</li> <li>e. Have you established functional states in order to keep your services operational under times of normal operation, duress/attack, and recovery? Do those requirements include planning for adequate capacity in order to maintain system availability? (ID.BE-5 PR.DS-4)</li> </ol> </li> </ol>	Based on the criticality of your services, your organization understands and prioritizes mission goals and infrastructure and how they relate to the industry. Your organization understands its role in the supply chain. Furthermore, a plan for continued availability and operation of your organization's assets is established.	Understands mission goals and infrastructure and how they relate to the industry; however, priorities are not adjusted accordingly which may impact availability and operation.	Functional states, mission goals, your organization's place in the supply chain, and infrastructure are not prioritized or understood.	

Protect	Awareness & Training	3. Does your organization have a security or risk awareness and training process in place? (PR.AT-1) a. Are roles and responsibilities clearly defined and understood by privileged users, third-party stakeholders (e.g. suppliers, customers, partners), senior executives, and physical and information security personnel? (PR.AT-2 PR.AT-3 PR.AT-4 PR.AT-5)	A thorough training program is implemented, and participation is tracked; there is an organization-wide awareness of established roles and responsibilities.	An informal training program is available for personnel to attend, and the organization publishes a guide for roles and responsibilities.	No training or awareness programs exist. Users must seek training on their own and there are no systems in place to track course completion.	Section Risk Total



### How does your organization protect data and systems?

Function	Category	Question to gauge risk posture	Satisfactory Response (Score of 1)	Medium Risk Response (Score of 2)	High Risk Response (Score of 3)	Score
Protect	Data Security	4. Who has access to data? (PR.DS1) a. How are least privilege and separation of duties managed? (PR.AC-4) b. How are access restrictions managed and maintained? (Username/password, RSA keys, Smartcards, remote access) (PR.AC-1, PR.AC-2, PR.AC-3) c. Do you validate the identity of personnel when issuing credentials and is their identity linked to those credentials? (PR.AC-6) d. Are your assets managed including removal, transferal and disposition? (PR.AC-2, PR.DS-3) e. Is data protected at rest and in transit? Is encryption used (i.e., SSL, TLS)? (PR.DS-1, PR.DS-2) f. Is the network segregated where appropriate? (PR.AC-5) g. Do you use a testing and development environment? (PR.DS-7) h. Does your organization consider cybersecurity when managing human resources? (PR.IP-11)	Data kept in encrypted on your organization's servers with security measures in place; two-factor authentication is required to access data; digital resources are managed; clear network segregation exists for sensitive data; development and testing environments are used.	Data kept in secure cloud storage; data access is reasonably controlled; users only utilize passwords to access data; digital resources are partially managed (e.g. removal is managed, however transfer is not); testing and development environments are considered but not segregated.	Data kept in low-security cloud storage or unprotected servers; personnel could call a help desk or another employee for account data without identity verification; resources are unmanaged; the network is not segregated; testing and/or development environments do not exist.	
	Identity Management & Access Control Information Protection					
Protect	Data Security	5. Is there a process in place to verify the integrity of software, firmware, hardware and information? (PR.DS-6, PR.DS-8)	Your organization has a rigorous verification process of software, firmware, hardware and information integrity.	Your organization has a verification process in place but is not always utilized in verifying software, firmware, hardware and information integrity.	There is no process in place to verify software, firmware, hardware and information integrity.	

<p><b>Protective Technology</b></p>	<p>6. How does your organization protect communications and networks? (PR.PT-4)</p>	<p>Your organization encrypts remote user traffic, and it understands, implements, and configures network monitoring devices such as IPS/IDS/Firewall at all boundary points and defined points within the system. Your organization utilizes VLANs where possible to segregate sensitive network data and traffic. TLS is utilized for internal and external web traffic. When implementing all of the methods listed above, your organization configures them with industry standard best practices for security.</p>	<p>Your organization implements many of the methods listed in the "satisfactory response" section above, however, it does not use industry standard best practices for configuring these methods. For example, your organization does not implement the following: deny all statements after explicit allow, configuration of remote sessions with a strong encryption method, using the most up to date version of TLS.</p> <p>Another response may be that your organization uses some of the methods listed above with industry standard best practices, but your organization does not have a well-structured defense-in-depth approach due to implementing only a few of the solutions instead of a larger suite.</p>	<p>You are unsure of the methods in place securing your organization's communications and networks. Technical protections are not well defined and documented.</p>
<p><b>Information Protection</b></p>	<p>7. Do you maintain your physical operating environment for organizational assets in line with established policies and regulations? (PR.IP-5)</p>	<p>Your organization implements policies and regulations for maintaining the physical operating environment and the established standards are consistently met.</p>	<p>Your organization has established policies and regulations for maintaining the physical operating environment however those standards are not consistently met.</p>	<p>There is no policy or regulations in place for maintaining the physical operating environment.</p>
<p><b>Protective Technology</b></p>	<p>8. How does your organization protect and restrict the use of removable media, and is it in line with policy? (PR.PT-2)</p>	<p>Your organization has a policy identifying how removable media should be used and it is communicated and well understood by all system users.</p>	<p>Your organization has a policy identifying how removable media should be used but it is not followed or understood by all system users.</p>	<p>No removable media policy exists for the use of removable devices. Removable media is not limited through technical means.</p>

<p><b>Protect</b></p>	<p>Data Security</p>	<p>9. Does your organization employ any additional processes to limit data leaks? (PR.DS-5)</p>	<p>Your organization has a comprehensive plan for managing and mitigating data leaks. Mitigation methods include many or all of the following: access control methods, established system configuration processes, encryption, intrusion detection, and end-user awareness.</p>	<p>Your organization has identified some data leak protection mechanisms, but the risk of data leaks is not reduced to an acceptable level using the industry standard methods.</p>	<p>There is no plan or mechanisms in place to control or mitigate data leaks.</p>	
<p><b>Protect</b></p>	<p>Information Protection</p>	<p>10. Does your organization continuously improve protection processes and is the effectiveness of those processes communicated to the appropriate stakeholders? (PR.IP-7 PR.IP-8)</p>	<p>Your organization has a well-defined review cycle for reviewing all protection processes. The review cycle includes an internal review and a continuous monitoring process. All inefficiencies discovered during review are documented, considered, and subjected to change and approval. The overall effectiveness is communicated with the appropriate parties.</p>	<p>Your organization has a review cycle for all protection processes, but that review process is not well defined or rarely followed and acted upon.</p>	<p>Your organization does not review protection processes.</p>	
<p><b>Section Risk Total</b></p>						

How are assets managed?

Function	Category	Question to gauge risk posture	Satisfactory Response (Score of 1)	Medium Risk Response (Score of 2)	High Risk Response (Score of 3)	Score
Identify Protect	Asset Management Technology	11. How are assets mapped, categorized and prioritized? (ID.AM) a. How are information flows mapped? (ID.AM-3) b. Do you document the use of external systems? (ID.AM-4) c. Are your organizational resources (e.g., hardware, devices, data, time, and software) prioritized? (ID.AM-5) d. Does your organization use audit logs and are they reviewed according to policy? (PR.PT-1)	Your organization has documented organizational data flows which include the use of any external systems. If any external systems are leveraged, the use case and information related to the external system is documented. Organizational resources including hardware, data, time, and software, are all prioritized based on their classification and criticality in relation to performing business objectives. Your organization has implemented the use of audit logs for assets/systems and the review of auditable events is performed as defined by your organization's policy.	Your organization has some documentation related to data flows and connections to external systems, but the documentation is not updated regularly. Some organizational resources are prioritized but many are left undefined.	There is no documentation around organizational data flows and the connections to any external systems. Organizational resources are not prioritized.	
Identify	Asset Management	12. How are assets tracked? (ID.AM) a. Is there a hardware inventory of devices and systems within your organization? (ID.AM-1) b. Do you keep a software inventory of platforms and applications within your organization? (ID.AM-2)	Your organization has an established inventory of all system assets which uses automated processes for updating and adding key information of those assets. Changes made to the inventory are monitored and/or only allowed by explicit personnel/processes.	Your organization's inventory is incomplete and/or there is key information missing for the listed assets. Inventory is updated at a monthly frequency or less often, and changes made to the inventory are not subjected to be performed by defined personnel and/or processes.	Your organization does not have an inventory of system assets, or changes to the inventory that have been documented are done at an ad-hoc frequency by undefined personnel.	

<p><b>Protect</b></p> <p>Information Technology</p>	<p>13. How are assets configured? (PR.IP)</p> <p>a. Is there a configuration baseline currently in use? (PR.IP-1)</p> <p>b. Is there a change management process? (PR.IP-3)</p> <p>c. Is there an SDLC process in place? (PR.IP-2)</p> <p>d. Is the principle of least functionality incorporated in your SDLC and current systems? (PR.PR-3)</p>	<p>Your organization uses a baseline configuration for all system assets. The configuration baseline and any changes made throughout the system are subjected to a well-defined SDLC and change management process (i.e. changes are authorized, tested, and approved). All configurations and changes consider the principle of least privilege.</p>	<p>Your organization uses baseline configurations for system assets, however the baselines are not well maintained or subjected to your SDLC or change management processes when maintenance or changes occur. Furthermore, the principle of least privilege is often an afterthought when configuring or making changes to system assets.</p>	<p>Your organization does not use a defined baseline configuration for system assets. There are not well-documented SDLC and change management processes and/or they are not implemented. Additionally, the least privilege principle is not considered in when making changes or configurations.</p>
<p><b>Protect</b></p> <p>Maintenance</p>	<p>14. Does your organization maintain and repair its assets in a timely manner and are such maintenance activities, including remote maintenance, logged and approved? (PR.MA-1 PR.MA-2)</p>	<p>Your organization has a thorough response team to address maintenance issues in a timely manner. Any maintenance activities are documented and approved including any remote maintenance sessions.</p>	<p>Your organization has personnel assigned to maintenance issues however, they are also tasked with other organizational processes, which in turn does not allow for a quick response time to maintenance issues. Remote activities are approved but not logged.</p>	<p>Your organization does not have defined personnel assigned to maintenance activities and there is no documentation of maintenance activities performed.</p>
<p><b>Protect</b></p> <p>Information Technology</p>	<p>15. How is data safely disposed of and/or destroyed? (PR.IP-6)</p> <p>a. Do assets undergo data sanitization? (PR.IP-6)</p>	<p>Your organization has a well-defined and understood policy describing the destruction/disposal of data and the sanitization of system assets containing organizational data. Disposal/destruction processes leverage third-party services providing certificates of device destruction and/or your organization takes elaborate measures to ensure devices are properly destroyed and/or disposed of. Your data sanitization process is consistent with the industry wide best practices.</p>	<p>Your organization has a policy describing how organizational assets and data are disposed of and sanitized. That policy is not well understood by all personnel performing disposal and/or sanitization processes.</p>	<p>Your organization does not have a process for the destruction/disposal of organizational assets, nor are you concerned with the sanitization of organizational assets containing data.</p>
<p><b>Section Risk Total</b></p>				

**How are vulnerabilities and suspicious activities detected and managed?**

Function	Category	Question to gauge risk posture	Satisfactory Response (Score of 1)	Medium Risk Response (Score of 2)	High Risk Response (Score of 3)	Score
Detect	Security Continuous Monitoring Processes	16. Does your organization perform scans for vulnerabilities, malicious code, and unauthorized mobile code? (DE.CM-4 DE.CM-5 DE.CM-8) a. Have you clearly defined scanning roles and responsibilities? (DE.DP-1) b. Are your scan definitions kept up to date? (DE.DP-5)	Daily or weekly scans are performed with strictly defined timelines for remediation and rigorous patch deployment procedures. Your organization uses a widely recognized scanning technology (i.e., Nessus, Qualys, or other major tools). Furthermore, your organization prioritizes vulnerabilities according to a severity score from CVSS, SCAP, or other vulnerability tracking standard.	Monthly or quarterly scans are performed with frequent slippage on remediation timelines. Roles and responsibilities are poorly defined for scanning and analysis. Scan definitions are updated on an ad hoc and not automated basis prior to scanning.	No scans performed. Remediation is performed, and patches are applied on an ad-hoc basis.	

<p><b>Date</b></p> <p><b>Resp</b></p> <p><b>ond</b></p>	<p><b>Security</b></p> <p><b>Continuo</b></p> <p><b>us</b></p> <p><b>Monitri</b></p> <p><b>ng</b></p> <p><b>Detecti</b></p> <p><b>on</b></p> <p><b>Processe</b></p> <p><b>s</b></p> <p><b>Anomalies &amp;</b></p> <p><b>Events</b></p> <p><b>Analysis</b></p> <p><b>Mitigation</b></p>	<p>17. How does your organization detect suspicious activity? (DE.DP) (DE.DP-1)</p> <p>a. Have you clearly defined detection roles and responsibilities? (DE.DP-1)</p> <p>b. Are detection activities compliant with requirements and communicated to appropriate parties? (DE.DP-2 DE.DP-4)</p> <p>c. Are detection processes tested and continuously improved? (DE.DP-3 DE.DP-5)</p> <p>d. Is the network, physical environment and personal activity monitored to detect cybersecurity events? (DE.CM-1 DE.CM-2 DE.CM-3)</p> <p>e. How is external service provider activity monitored? (DE.CM-6)</p> <p>f. How are unauthorized personnel, connections, devices, and software monitored? (DE.CM-7)</p> <p>g. Are multiple data sources and logical and/or physical sensors considered when reviewing an event? (DE.AE-3)</p> <p>h. When a notification from a detection system is received, does your organization investigate, contain, mitigate and categorize the incident consistent with the response plan? (RS.AN-1 RS.AN-4 RS.MI-1 RS.MI-2)</p>	<p>Your organization has a strong detection system that monitors the following for cybersecurity events: network, physical environment, personnel and external service providers. Furthermore, your organization continuously monitors your system and physical infrastructure for unauthorized personnel, connections, devices or software. Individuals are notified and held accountable for detection activities as per the roles and responsibilities established by a policy document or responsibility matrix. A notification is sent for any suspicious activity, and dependent on roles and responsibilities, individuals work to resolve the issue per the response plan in a timely manner. The detection process is regularly tested and improved.</p>	<p>While a detection system is in place, your organization does not have well-defined roles and responsibilities for detection. Accountability is not established for specific detection activities and the detection process is not frequently updated. Cybersecurity events are resolved, but the response plan is not followed.</p>	<p>Your organization does not have a system or process for detecting suspicious activity. Identifying incidents is reliant upon individuals and disparate efforts across the organization.</p>	<p><b>Section Risk Total</b></p>
<p><b>Date</b></p> <p><b>ct</b></p>	<p><b>Anomalies &amp;</b></p> <p><b>Events</b></p>	<p>18. Does your organization establish and manage a baseline of network operations and expected data flows for users and systems? (DE.AE-1)</p> <p>a. Is incident alerting in place for any event falling outside of the established threshold? (DE.AE-5)</p> <p>b. Are detected events analyzed to determine attack targets and methods, as well as the impact those events may have on the system? (DE.AE-2 DE.AE-4)</p>	<p>Your organization continuously maintains a baseline for expected network operations, and user and system data flows. An automated incident alerting system is in place and alerting thresholds are set for when deviations occur from the baseline. When an event occurs, the attack methods and targets are analyzed, and the impact of the event is ascertained.</p>	<p>A baseline for expected network operations, user and system data flows are established. The baseline and data flows are not, however managed or updated on a regular basis. There is a systematic alerting system in place for when deviations from this baseline occur. Additionally, your organization has no formalized process of how events are analyzed.</p>	<p>There is no systematic incident alerting established, and incidents are investigated and resolved on an ad-hoc basis.</p>	

How are security incidents handled?

Function	Category	Question to gauge risk posture	Satisfactory Response (Score of 1)	Medium Risk Response (Score of 2)	High Risk Response (Score of 3)	Score
Identify, Protect & Respond	Information Protection Communications Response Planning Supply Chain Risk Management	19. Is there an incident response plan and when is it executed? (RS.RP-1 PR.IP-9)	There is an extensive incident response plan with clearly defined roles and responsibilities, frequent testing with internal and external stakeholders, early detection, and constant updates.	There is an incident response plan, but it is out-of-date and infrequently tested. Roles and responsibilities are not understood by all personnel that partake in the incident response process.	There is no established incident response plan and/or processes and procedures documented in the plan are not used in the actual response to incidents.	
		a. How often is the plan tested? (PR.IP-10) b. Do personnel understand their role and the actions required of them when a response is needed? (RS.CO-1) c. Is response planning and testing conducted in coordination with stakeholders, including critical suppliers and providers? (RS.CO-4 ID.SC-5)				
Respond	Communications	20. Are security incidents reported? (RS.CO-2)	There is an established criteria or standard for the reporting of events, that is understood and followed by your organization's personnel. Those reported events are documented which include records of remediation timelines and disclosure to any internal or external stakeholders.	There is an ad-hoc response to reporting security incidents. Information disclosure is not always performed with internal or external stakeholders when needed.	There is no process to report security incidents. Incidents are handled on an ad hoc basis.	
Recover		a. Are recovery activities communicated to the appropriate personnel and is the information shared consistent with the response plan? (RC.CO-3 RS.CO-3) b. Does your plan include disclosure instructions regarding other required parties for notification of incidents, including any external stakeholders, as necessary? (RC.CO-1 RC.CO-2 RS.CO-5)				



<p><b>Identify, Protect &amp; Recover</b></p> <p>Information Protection Recovery Planning Supply Chain Risk Management</p>	<p>21. Is there a recovery plan in place and what is the timeline for restoration? (RC.RP-1, PR.IP-9)</p> <p>a. How often is the plan tested? (PR.IP-10)</p> <p>b. Is recovery planning and testing conducted with critical suppliers and providers? (ID.SC-5)</p> <p>c. Does your organization have backups in place to restore from and do you test them? (PR.IP-4)</p>	<p>There is an extensive recovery response plan with clearly defined roles and responsibilities, restoration timeline, and it is frequently tested with internal and external stakeholders. Incremental and/or full backups of information are regularly performed and the backup and restore mechanism is tested at least on at least an annual basis.</p>	<p>A recovery plan exists, but it is not up-to-date and is not frequently tested. Backups of information are performed; however, the restoration process is not tested periodically.</p>	<p>There is no recovery plan in place and an untested backup mechanism is utilized. Backups are not available for all systems.</p>
<p><b>Respond</b></p> <p>Analysis Mitigations Improvements</p>	<p>22. Are the response and recovery processes updated as incidents occur? (RS.IM-2, RC.IM-2)</p> <p>a. Are lessons learned incorporated? (RS.IM-1, RC.IM-1)</p> <p>b. Is a root-cause analysis performed for each incident and is the impact determined? (RS.AN-2, RS.AN-3)</p> <p>c. Does your organization mitigate newly identified vulnerabilities and when resolution is not possible, is the accepted risk documented? (RS.MI-3)</p>	<p>The response and recovery strategies are updated incorporating any lessons learned and takeaways from a root cause analysis. Your organization records vulnerabilities that cannot be mitigated and documents them as an accepted risk.</p>	<p>Forensics are not frequently performed to determine the root cause of an incident. As such, the response and recovery strategies are not updated in the aftermath of new incidents, but rather, on an ad-hoc basis.</p>	<p>Response and recovery plans are not updated as incidents occur. Root cause is often not determined or documented as part of incident response.</p>
<p><b>Section Risk Total</b></p>				

How do you manage security risks?

Function	Category	Question to gauge risk posture	Satisfactory Response (Score of 1)	Medium Risk Response (Score of 2)	High Risk Response (Score of 3)	Score
Identify Protect	Risk Management Strategy Governance Risk Assessment Information Protection	23. Does your organization have a process to manage risk including cybersecurity risk? (ID.RM-1 (D.GV-4)) a. Do you identify and document both internal and external threats, vulnerabilities, the likelihood of impact and the potential impact to your organization? Do you document the associated risk levels? (ID.RA-1 (D.RA-3 (D.RA-4 (D.RA-5)) b. Do you use forums or other shared sources to gather cyber threat or vulnerability information? (D.RA-2) c. Have you implemented a plan to manage vulnerabilities? (PR.IP-12) d. Does your organization have a clearly defined and documented risk tolerance taking into consideration infrastructure and industry risk? (ID.RM-2 (D.RM-3)) e. Are resources prioritized to high risk items? (D.RA-6)	The risk management process is kept up-to-date and is extensively used in security decisions. Your organization has documented its risk tolerance and there is good external and internal threat modeling with impact analysis. A plan is established to manage vulnerabilities based on the risk analysis and tolerance levels. Furthermore, there is good prioritization of resources, and priorities are adjusted when the level of risk changes, which allows for resources to be dedicated to high risk areas as appropriate.	The risk management process is infrequently updated, and it is used for some security decisions. There is a weakly defined risk tolerance and resources are not always prioritized per risk. As such, high risk areas may not receive prioritization when allocating resources	There is no risk management, resources are not allocated toward high-priority incidents when they occur, and there is little to no documentation or implementation to assist in the case of an incident. Stakeholders have no or little idea of current threats facing the organization.	
	Supply Chain Risk Management	24. Has your organization established a process to manage cyber supply chain risk, including identifying, prioritizing and assessing both suppliers and partners of critical systems and services? (ID.SC-1 (D.SC-2)) a. Does your organization monitor your suppliers and partners to evaluate that they are meeting obligations and your information security objectives as contracted? (ID.SC-3 and ID.SC-4)	The cyber supply chain risk management process is kept up-to-date and is used in supply chain decisions. Cyber supply chain risk tolerances are appropriately defined. On at least an annual basis, your organization reviews audit summaries or conducts independent evaluations of suppliers and partners to validate that all contracted obligations are met and that the suppliers and partners have implemented measures to meet your organization's information security and cyber supply chain management standards.	A cyber supply chain risk management process exists, but it is infrequently updated and is not used for all cyber supply chain security decisions. As such, prioritization of resources is not always considered. Information security and cyber supply chain management standards are communicated to the suppliers and partners; however, they are not formally contracted nor are the partners and suppliers regularly monitored to determine whether they are meeting obligations.	No risk management processes for cyber supply chain exist. Your organization has not performed an analysis to identify suppliers and partners of your critical systems, components and services, and thus priorities have not been adjusted accordingly with the presented risk.	