NEW YORK STATE MODEL DATA PRIVACY AGREEMENT FOR EDUCATIONAL AGENCIES

Saratoga Springs City School District

and

Adirondack School Portraits

This Data Privacy Agreement ("DPA") is by and between the Saratoga Springs City School District ("EA"), an Educational Agency, and Adirondack School Portraits ("Contractor"), collectively, the "Parties".

ARTICLE I: DEFINITIONS

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

1. **Breach:** The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information in a manner not permitted by State and federal laws, rules and regulations, or in a manner which compromises its security or privacy, or by or to a person not authorized to acquire, access, use, or receive it, or a Breach of Contractor's security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personally Identifiable Information.
2. **Commercial or Marketing Purpose:** means the sale, use or disclosure of Personally Identifiable Information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of Personally Identifiable Information for advertising purposes; or the sale, use or disclosure of Personally Identifiable Information to develop, improve or market products or services to students.
3. **Disclose:** To permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written or electronic, whether intended or unintended.
4. **Education Record:** An education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
5. **Educational Agency**: As defined in Education Law 2-d, a school district, board of cooperative educational services, school, charter school, or the New York State Education Department.
6. **Eligible Student:** A student who is eighteen years of age or older.
7. **Encrypt or Encryption**: As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304, means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable

form in which there is a low probability of assigning meaning without use of a confidential process or key.

8. **NIST Cybersecurity Framework**: The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
9. **Parent:** A parent, legal guardian or person in parental relation to the Student.
10. **Personally Identifiable Information (PII):** Means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g , and Teacher or Principal APPR Data, as defined below.
11. **Release:** Shall have the same meaning as Disclose.
12. **School:** Any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law § 3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law § 4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.
13. **Student:** Any person attending or seeking to enroll in an Educational Agency.
14. **Student Data:** Personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g.
15. **Subcontractor:** Contractor's non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.
16. **Teacher or Principal APPR Data**: Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d.

ARTICLE II: PRIVACY AND SECURITY OF PII

1. **Compliance with Law.**

   In order for Contractor to provide certain services ("Services") to the EA pursuant to a contract dated **7/01/2022 – 6/30/2023** ("Service Agreement"); Contractor may receive PII regulated by several New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20

U.S.C. 1400 et seq. (34 CFR Part 300); New York Education Law Section 2-d; and the Commissioner of Education's Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements of New York law. Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federal and local laws, rules and regulations.

2. **Authorized Use.**
   Contractor has no property or licensing rights or claims of ownership to PII, and Contractor must not use PII for any purpose other than to provide the Services set forth in the Service Agreement. Neither the Services provided nor the manner in which such Services are provided shall violate New York law.

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

4. **EA's Data Security and Privacy Policy**
   State law and regulation requires the EA to adopt a data security and privacy policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST Cyber Security Framework. Contractor shall comply with the EA's data security and privacy policy and other applicable policies.

5. **Right of Review and Audit.**
   Upon request by the EA, Contractor shall provide the EA with copies of its policies and related procedures that pertain to the protection of PII. It may be made available in a form that does not violate Contractor's own information security policies, confidentiality obligations, and applicable laws. In addition, Contractor may be required to undergo an audit of its privacy and security safeguards, measures and controls as it pertains to alignment with the requirements of New York State laws and regulations, the EA's policies applicable to Contractor, and alignment with the NIST Cybersecurity Framework performed by an independent third party at Contractor's expense, and provide the audit report to the EA. Contractor may provide the EA with a recent industry standard independent audit report on Contractor's privacy and security practices as an alternative to undergoing an audit.

6. Contractor's Employees and Subcontractors.

(a) Contractor shall only disclose PII to Contractor's employees and subcontractors who need to know the PII in order to provide the Services and the disclosure of PII shall be limited to the extent necessary to provide such Services. Contractor shall ensure that all such employees and subcontractors comply with the terms of this DPA.

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

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

(d) Contractor shall take full responsibility for the acts and omissions of its employees and subcontractors.

(e) Contractor must not disclose PII to any other party unless such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the EA of the court order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the PII is disclosed, unless such disclosure to the EA is expressly prohibited by the statute, court order or subpoena.

7. Training.

Contactor shall ensure that all its employees and Subcontractors who have access to PII have received or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access.

8. Termination

The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its sub-contractors retain PII or retain access to PII.

9. Data Return and Destruction of Data.

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

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

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

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

10. Commercial or Marketing Use Prohibition.

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

11. Encryption.

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

12. Breach.

(a) Contractor shall promptly notify the EA of any Breach of PII without unreasonable delay no later than seven (7) business days after discovery of the Breach. Notifications required pursuant to this section must be in writing, given by personal delivery, e-mail transmission (if contact information is provided for the specific mode of delivery), or by registered or certified, and must to the extent available, include a description of the Breach which includes the date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Contractor's investigation; and the contact information for representatives who can assist the EA. Notifications required by this section must be sent to the EA's District Superintendent or other head administrator with a copy to the Data Protection Office. Violations of the requirement to notify the EA shall be subject to a civil penalty pursuant to Education Law Section 2-d. The Breach of certain PII protected by Education Law Section 2-d may subject the Contractor to additional penalties.

(b) Notifications required under this paragraph must be provided to the EA at the following address:

David L'Hommedieu
Assistant Superintendent of Information Technology and Operational Innovation & Data Protection Officer
3 Blue Streak Blvd.
Saratoga Springs, NY 12866
D_lhommedieu@saratogaschools.org

13. Cooperation with Investigations.

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

14. **Notification to Individuals.**

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

15. **Termination.**

The confidentiality and data security obligations of the Contractor under this DPA shall survive any termination of this DPA but shall terminate upon Contractor's certifying that it has destroyed all PII.

ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS

1. **Parent and Eligible Student Access.**

Education Law Section 2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student's Student Data stored or maintained by the EA. To the extent Student Data is held by Contractor pursuant to the Service Agreement, Contractor shall respond within thirty (30) calendar days to the EA's requests for access to Student Data so the EA can facilitate such review by a Parent or Eligible Student, and facilitate corrections, as necessary. If a Parent or Eligible Student contacts Contractor directly to review any of the Student Data held by Contractor pursuant to the Service Agreement, Contractor shall promptly notify the EA and refer the Parent or Eligible Student to the EA.

2. **Bill of Rights for Data Privacy and Security.**

As required by Education Law Section 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Service Agreement are included as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. Contractor shall complete and sign Exhibit B and append it to this DPA. Pursuant to Education Law Section 2-d, the EA is required to post the completed Exhibit B on its website.

ARTICLE IV: MISCELLANEOUS

1. **Priority of Agreements and Precedence.**

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

2. **Execution.**

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

EDUCATIONAL AGENCY: **Saratoga Springs CSD**	**CONTRACTOR:** Adirondack School Portraits
BY: ***[Signature]***	BY: ***[Signature]*** Joseph J. Marcelletti Sr
[Printed Name] DAVID L'HOMMEDIEU	***[Printed Name]*** Joseph J. Marcelletti Sr.
[Title] Assistant Superintendent	**[Title]** President
Date: 11-9-23	Date: **10/20/2023**

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

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.

3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.

4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.

5. A complete list of all student data elements collected by NYSED is available at www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the EA at sscsd_dpo@saratogaschools.org. (ii) Complaints may also be submitted to the NYS Education Department at www.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474-0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.

8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

CONTRACTOR : Adirondack School Portraits	
[Signature]	
[Printed Name]	Joseph J. Marcelletti Sr.
[Title]	President
Date:	10/20/2023

EXHIBIT B

BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY - SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner's Regulations, the Educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

Name of Contractor	**Adirondack School Portraits**
Description of the purpose(s) for which Contractor will receive/access PII	**Adirondack School Portraits acknowledges that the student information is provided by the District solely for student yearbook portraits, portrait package purchasing, student photo identification cards and for the purpose of communicating picture day details.**
Type of PII that Contractor will receive/access	Check all that apply: **X** Student PII □ APPR Data
Contract Term	***Contract Start Date: July 1, 2023*** ***Contract End Date: June 30, 2024***
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) □ Contractor will not utilize subcontractors. **X Contractor will utilize subcontractors.**
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: **• Securely transfer data to EA, or a successor contractor at the EA's optionand written discretion, in a format agreed to by the parties, or Securely delete and destroy data as may be directed by written request from District.**
Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.

Secure Storage and Data Security	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply) □ Using a cloud or infrastructure owned and hosted by a third party. □ Using Contractor owned and hosted solution X Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: PII data is only accessed by key employees necessary to perform our obligations under this contract. PII Data can only be accessed via an on-site internal server with no internet access and password protected for management usage only.
Encryption	Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: **PII data is only accessed by employees necessary to perform our obligations under this contract. Data will be encrypted while in motion. Password protected at rest on internal server without internet accessibility.**

CONTRACTOR : Adirondack School Portraits	
[Signature] Joseph J. Marcelletti SR.	
[Printed Name] JOSEPH J. MARCELLETTI SR.	
[Title] PRESIDENT	
Date: *October 20, 2023*	

EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security andprivacy contract requirements over the life of the Contract.	All concerns related to data protection can be referred to Joseph Marcelletti Sr. 518-792-7919 ext 104 jmarcel7@nycap.rr.com or Joseph Marcelletti Jr: 518-792-7919 ext 105 jmarch@bielmar.com
2	Specify the administrative, operational and technical safeguardsand practices that you have in place to protect PII.	Technical support contact is Kevin Moon 518-792-7919 ext 108 kevin@bielmar.com
3	Address the training received by your employees and any subcontractors engaged in the provision of services under theContract on the federal and state laws that govern the confidentiality of PII.	Employees are instructed and strictly prohibited to release any student information or photos to a third party without the prior written/digital consent of the school administrator, principal or parent(s) of the student or, if 18 years of age or older, the student.
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	The student information that has been provided to us is solely for production of student yearbook portraits, portrait package purchasing, student photo identification cards and for the purpose of communicating picture day details to parents.
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to theEA.	The staff at Saratoga City School District that monitors this contract will be notified via email of any security breaches that involve student/staff PII .
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	We agree not to retain student identification numbers assigned by the District after completing our services relative to student services. All data will be wiped from our database at the expiration of the portrait services agreement upon the written direction of the Saratoga City School District.
7	Describe your secure destruction practices and how certificationwill be provided to the EA.	We would use a standard "delete file" instruction to our local server however, if instructed by the district, we would use a US DoD 5220.22-M standard with 3 pass system. Additionally we use a secure shredding process that physically destroys all old media. Contractor will provide EA with certification of such destruction.

8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Contractor will implement the data protection and security requirements outlined in 8 NYCRR Part 121, and include EA's Parents Bill of Rights and Supplemental Information to the Service Agreement
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chartbelow.	

EXHIBIT C.1 – NIST CSF TABLE

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

Function	Category	Contractor Response
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	IT Department shall: a. Identify and select the following types of information system accounts to support organizational missions and business functions: individual, system, emergency. b. Assign account managers for information system accounts. c. Establish conditions for group and role membership. d. Specify authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account. e. Require approvals of Company IT Department for requests to create information system accounts. f. Create, enable, modify, disable, and remove information system accounts in accordance with approved procedures. g. Monitor the use of information system accounts. h. Notify the company IT Department when accounts are no longer required, when users are terminated or transferred, and when individual information system usage or need-to-know changes. i. Authorize access to the information system based on a valid access authorization or intended system usage.
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	As a provider of photographic services, Adirondack School Portraits core objective is to provide a high quality product to the schools and business that we serve. In order to accomplish this, our business utilizes many software applications that house valuable information for enhancing the creation and distribution of photographic packages. These systems may reside on site or are hosted with outside partners. Some systems and software titles are procured from outside vendors for our operations. Our business does develop propriety software and applications. These systems are utilized only by employees of our business. Adirondack School Portraits requires that any subcontractor who may have access to PII are bound by written agreement to at a minimum, the security requirements of the Contract.

	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**Adirondack School Portraits will comply with all applicable laws and regulations, including:** **Federal and State Laws** **Industry Regulations** **Contracts** **Insurance Policy Requirements** **Information security roles & responsibilities will be coordinated and aligned with internal roles and external partners.** **Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, must be understood and managed. Governance and risk management processes will address cybersecurity risks.** **The Adirondack School Portrait ecommerce site utilizes the latest TLS/SSL encryption and server security. All student images stored online use a 10 key high entropy pass code. Embedded within the jpg metadata of the gallery image is a unique identifier used to locate the image in the lab. This unique identifier is a random 10 key high entropy pass code that does not relate to a school or any personal information. All information transferred from our ecommerce site to the lab to produce an order is done via an encrypted direct FTP connection For added safety, no personal identifying information is ever transmitted to the image server.**
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**Adirondack School Portraits agrees to notify the district immediately upon the detection and/or notification of a data breach on any server housing district information at rest. This data is only stored on an internal server with no internet access and password protected. Only limited key management personnel have access and feel the risk factor is minimal.**
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**At Adirondack School Portraits information security risk management takes into account vulnerabilities, threat sources, and security controls that are planned or in place. These inputs are used to determine the resulting level of risk posed to information, systems, processes, and individuals that support business functions.** **While risk management and related assessment activities can take many forms (e.g., formal risk assessment, audits, security reviews, configuration analysis, vulnerability scanning and testing), all are aimed at the same goal - identifying and acting on risk to improve overall security posture. It is for this reason we have chosen to forgo cloud based storage platforms and secure all student data on internal storage units, which are not connected to the internet and can only be accessed via password protection and by limited management personnel.**
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	**Adirondack School Portraits shall have in place alternate sources of vendors and suppliers of materials required to provide the services contracted for to insure delivery of goods and services contracted for over the period of this contract and succeeding periods.**

Function	Category	Contractor Response
PROTECT (PR)		
	Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	PHYSICAL SECURITY CONTROLS Provide initial and ongoing training in the employment and operation of physical security controls; physical security controls include, for example, physical access control devices, physical intrusion alarms, and facility smoke/fire monitoring.
	Awareness and Training (PR.AT): The organization's personnel and partners areprovided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	These policies are applicable to all departments and users of IT resources and assets at Adirondack School Portraits 1. SECURITY AWARENESS TRAINING 2. SECURITY AWARENESS | INSIDER THREAT 3. PHYSICAL SECURITY CONTROLS 4. SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, andavailability of information.	**Information Statement** <u>Organizational Security.</u> Adirondack School Portraits will designate an individual to be responsible for the risk management function. <u>Executive management is responsible for:</u> 1. evaluating and accepting risk on behalf of the company. 2. identifying information security responsibilities and goals and integrating them into relevant processes; 3. supporting the consistent implementation of information security policies and standards; 4. supporting security through clear direction and demonstrated commitment of appropriate resources; 5. implementing the process for information asset identification, handling, use, transmission, and disposal based on information classification and categorization; 6. determining who will be assigned and serve as information owners while maintaining ultimate responsibility for the confidentiality, integrity, and availability of the data; 7. participating in the response to security incidents; 8. complying with notification requirements in the event of a breach of private information; 9. communicating requirements of this policy and the associated standards, including the consequences of non-compliance, to the workforce and third parties, and addressing adherence in third party agreements. <u>Designated security representative is responsible for:</u>

Data Security (PR.DS):

Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, andavailability of information

1. **maintaining familiarity with business functions and requirements;**
2. **maintaining an adequate level of current knowledge and proficiency in information security**
3. **evaluating and understanding information security risks and how to appropriately manage those risks;**
4. **representing and assuring security architecture considerations are addressed;**
5. **participating in the development of corporate policies and standards that considers the company's needs;**
6. **promoting information security awareness.**

<u>IT management is responsible for:</u>

1. **supporting security by providing clear direction and consideration of security controls in the data processing infrastructure and computing network(s) which support the information owners;**
2. **providing resources needed to maintain a level of information security control consistent with this policy;**
3. **identifying and implementing all processes, policies and controls relative to security requirements defined by the business and this policy;**
4. **implementing the proper controls for information owned based on the classification designations;**
5. **implementing business continuity and disaster recovery plans.**

<u>The Workforce is responsible for:</u>

1. **understanding the baseline information security controls necessary to protect the confidentiality, integrity and availability of information entrusted;**
2. **protecting information and resources from unauthorized use or disclosure;**
3. **protecting personal, private, sensitive informationfrom unauthorized use or disclosure;**

<u>Executive management is responsible for:</u>

1. **providing in-house expertise as security consultants as needed;**
2. **developing the security program and strategy, including measures of effectiveness;**
3. **establishing and maintaining enterprise information security policy and standards;**
4. **assessing compliance with security policies and standards;**
5. **providing incident response coordination and expertise;**
6. **PII must not be made available without appropriate safeguards approved by management.**

<u>Separation of Duties</u>

a. **To reduce the risk of accidental or deliberate system misuse, separation of duties and areas of responsibility must be implemented where appropriate.**

b. **Whenever separation of duties is not technically feasible, other compensatory controls must be implemented, such as monitoring of activities, and management supervision.**

Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systemsand assets.

1. **BASELINE CONFIGURATION**

   IT Department shall:

   a. **Develop, document, and maintain under configuration control, a current baseline configuration of information systems.**

   b. **Review and update the baseline configuration of the information system Annually**

   c. **Retain one previous version of baseline configurations of information systems to support rollback.**

2. **CONFIGURATION CHANGE CONTROL**

   IT Department shall:

   a. **Determine the types of changes to the information system that are configuration-controlled.**

   b. **Review proposed configuration-controlled changes to the information system and approve or disapprove such changes with explicit consideration for security impact analyses.**

   c. **Document configuration change decisions associated with the information system.**

   d. **Implement approved configuration-controlled changes to the information system.**

   e. **Retain records of configuration-controlled changes to the information system for 2 Years**

   f. **Audit and review activities associated with configuration-controlled changes to the information system.**

   g. **Test, validate, and document changes to the information system before implementing the changes on the operational system.**

3. **SECURITY IMPACT ANALYSIS**

   IT Department shall:

   a. **Analyze changes to the information system to determine potential security impacts prior to change implementation.**

	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	CONTROLLED MAINTENANCE IT Department shall: a. Schedule, perform, document, and review records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications b. Approve and monitor all maintenance activities c. Sanitize equipment to remove all information from associated media prior to removal from facilities for off-site maintenance or repairs. d. Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions. e. Include IT and system owner's defined maintenance-related information in maintenance records. MAINTENANCE TOOLS IT Department shall: a. Ensure that system owners and IT approve, control, and monitor information system maintenance tools. b. Inspect the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications. c. Check media containing diagnostic and test programs for malicious code before the media are used in the information system. 1. NON-LOCAL MAINTENANCE IT Department shall: a. Approve and monitor non-local maintenance and diagnostic activities. b. Allow the use of non-local maintenance and diagnostic tools only as consistent with policy and documented in the security plan for the information system. c. Employ strong authenticators in the establishment of non-local maintenance and diagnostic sessions. d. Maintain records for non-local maintenance and diagnostic activities. e. Terminate session and network connections when non-local maintenance is completed. f. Document in the security plan for the information system, the policies and procedures for the establishment and use of non-local maintenance and diagnostic connections. 2. MAINTENANCE PERSONNEL IT Department shall: a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel. b. Ensure that non-escorted personnel performing maintenance on the information system have required access authorizations. c. Designate personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations. 3. TIMELY MAINTENANCE IT Department shall:

	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	**a. Obtain maintenance support and/or spare parts for information systems as agreed upon within the service level agreement between IT and the system owner.** **COMPLIANCE** **Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.**
	Protective Technology (PR.PT): Technical security solutions are managed to ensurethe security and resilience of systems andassets, consistent with related policies, procedures, and agreements.	**1. MEDIA ACCESS:** **IT through direction from departments shall:** **a. Restrict access to all digital and non digital media to all staff without a direct need to access the media to conduct their jobs.** **b. Mark information system media indicating the distribution limitations, handling caveats, and applicable security markings of digital and non-digital information media.** **2. MEDIA STORAGE** **IT Department shall:** **a. Specify staff to physically control and securely store media within defined controlled areas.** **b. Protect information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.** **3. MEDIA TRANSPORT** **IT Department Shall:** **a. Protect and control media during transport outside of controlled areas.** **b. Maintain accountability for information system media during transport outside of controlled areas.** **c. Document activities associated with the transport of information system media.** **d. Restrict the activities associated with the transport of information system media to authorized personnel.** **4. MEDIA SANITIZATION** **IT Department shall:** **a. Sanitize prior to disposal, release out of organizational control, or release for reuse in accordance with applicable federal and organizational standards and policies.** **b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.** **COMPLIANCE** **Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.**

DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	FLAW REMEDIATION IT Department shall: a. Identify, report, and correct information system flaws. b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation. c. Install security-relevant software and firmware updates 7 days of the release of the updates, unless released as a critical update. d. Incorporate flaw remediation into the configuration management process. MALICIOUS CODE PROTECTION IT Department shall: a. Employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code. b. Update malicious code protection mechanisms whenever new releases are available in accordance with configuration management policy and procedures. c. Configure malicious code protection mechanisms to: i. Perform periodic scans of the information system continuous and real-time scans of files from external sources at endpoint; network entry/exit points as the files are downloaded, opened, or executed in accordance with the security policy. ii. Block malicious code; quarantine malicious code; send alert to administrator; in response to malicious code detection. iii. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. 1. INFORMATION SYSTEM MONITORING IT Department shall: a. Monitor the information system to detect: i. Attacks and indicators of potential attacks. ii. Unauthorized local, network, and remote connections. b. Identify unauthorized use of the information system through defined techniques and methods. c. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion. d. Heighten the level of information system monitoring activity whenever there is an indication of increased risk to operations and assets, individuals, other organizations, or based on law enforcement information, intelligence information, or other credible sources of information. e. Obtain legal opinion with regard to information system monitoring activities in accordance with applicable state and federal laws, directives, policies, or regulations. f. Provide information system monitoring information to authorized personnel or business units as needed. SECURITY ALERTS, ADVISORIES, AND DIRECTIVES IT Department shall: a. Generate internal security alerts, advisories, and directives as deemed necessary. b. Disseminate security alerts, advisories, and directives to IT Department manager and ownership. c. Implement security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance. SPAM PROTECTION IT Department shall: a. Employ spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages.

Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.

- b. **Update spam protection mechanisms when new releases are available in accordance with the configuration management policy and procedures.**
- c. **Manage spam protection mechanisms centrally.**
- d. **Ensure information systems automatically update spam protection mechanisms.**

ERROR HANDLING

IT Department shall:

a. **Ensure the information system:**

- i. **Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.**
- ii. **Reveals error messages only to IT Manager and ownership**

2. **INFORMATION HANDLING AND RETENTION**

IT Department shall:

a. **Handle and retain information within the information system and information output from the system in accordance with applicable state and federal laws, directives, policies, regulations, standards, and operational requirements.**

Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.

Information Statement

As per the Information Security Policy, all systems must be scanned for vulnerabilities. In addition, each system must be inventoried and have an individual or group assigned responsibility for maintenance and administration.

Types of Scans

type of vulnerability scans appropriate for a given target depends on the target type (i.e., hardware, software, source code) and the target's location (i.e., internal or external to the network). The table below lists the types of vulnerability scans required by this standard.

4

Type	Description
External Infrastructure Scan	**Scans of the perimeter of networks or any externally available hosted infrastructure to identify potential vulnerabilities in Internet accessible IT infrastructure.**
Internal Infrastructure Scan	**Scans of IT infrastructure on protected networks or any hosted infrastructure to identify potential vulnerabilities.**
"Lite" Web Application Scan	**Cursory unauthenticated scans of externally facing production web applications to identify security vulnerabilities.**
In-depth Web Application Scan	**When implemented, authenticated in-depth scans ofweb applications to identify security vulnerabilities.**
Application Source Code Analysis	**Scans of application source code run during development to identify problems in the code that could cause potential vulnerabilities.**

Scanning

IT Mangager is responsible for confirming that vulnerability scans are conducted.

	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures	**Any approved scanning tool must be able to provide remediation suggestions and be able to associate a severity value to each vulnerability discovered based on the relative impact of the vulnerability to the affected system.** **As per the Information Classification Standard, scan reports are classified with moderate confidentiality and moderate integrity and should be protected as such.** **Network and system administrators must provide sufficient access to allow the vulnerability scan engine to scan all services provided by the system. No devices connected to the network shall be specifically configured to block vulnerability scans from authorized scanning engines.** **Scans must be performed within the system development life cycle while in pre-deployment environments, when deployed into the target implementation environment, and periodically thereafter as specified below:** **a. Pre-deployment scans occur prior to the move of the system or web application to the target implementation environment:** **1. All systems must undergo an authenticated internal infrastructure scan, where technically feasible or required, before being deployed to the target implementation environment.** **2. When source code is available, applications must undergo source code scanning before the updated code moves into the target implementation environment if there has been a change to application code.** **3. Scans must be authenticated when the application requires authentication before being deployed into the target implementation environment or into an environment that is externally accessible. When authentication is required to access the application, scans must be run with authenticated access at each access level (e.g., user, admin) supported by the application, except where limitations in the tool prevent authenticated scanning. Any web application vulnerability discovered must be remediated or determined to be a false positive or insignificant risk by the ISO/designated security representative, prior to the system being placed into the target implementation environment.** **4. Any system or application deployed to its target implementation environment with un-remediated vulnerabilities must have a formal remediation plan and the documented approval of the executive responsible for risk management or their designee.** **b. Implementation scans occur the first time a system or web application is moved to its target implementation environment:** **1. Systems must be scanned immediately upon being placed into the target implementation environment with an authenticated internal infrastructure scan, where technically feasible or required. If the system is accessible from the Internet or an external network, then the system must be scanned with an external infrastructure scan.** **2. Web applications must be scanned within the first month of being placed into the target implementation environment. An authenticated in-depth web application scan is required if feasible, but at minimum a "lite" web application scan is required. Sensitivity and criticality of the application must be considered when determining the schedule for the initial implementation scan.**

Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures

c. Recurring Scans: After the initial scan in the target implementation environment, the frequency of scans are to occur according to the system or application's risk rating (see Table 2).

1. When performing internal infrastructure scans on systems built using a shared image, such as workstations, scans may be run on a sampling of systems but the sample set must vary from scan to scan.
2. Web applications in production are required to undergo recurring scans. At minimum, web applications in production are required to undergo recurring "lite" application scans.
3. All vulnerabilities found during scans must be addressed as per the remediation section below.

Determine Risk Rating and Frequency of Scans

The risk that vulnerabilities pose to systems and applications is based on the likelihood of a vulnerability being exploited and the impact if the confidentiality, integrity or availability of the information assets were compromised. The likelihood of a vulnerability being exploited is increased in direct relation to the system's or application's accessibility from other systems.

The impact to the information assets is based on the asset's information classification (see Information Classification Standard). Impact (i.e., high, moderate or low) if the confidentiality, integrity or availability is compromised must be considered and the highest individual impact rating for confidentiality, integrity or availability utilized within the table below.

Table 2: RISK RATING

Impact (Confidentiality, Integrity, Availability)	Exposure	
	Systems with no network connectivity to production data	Systems with network connectivity to production data (not internet facing)
High	Medium	High
Medium	Low	Medium
Low	Low	Low

Minimum frequency of scans is dependent on the risk rating. Systems without a risk rating must be scanned as if they had a risk rating of "High" until they are rated.

TABLE 3: FREQUENCY OF SCANS

Risk Rating	Frequency
Infrastructure scans	
High	Monthly

Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures

Medium	Quarterly
Low	Semi-annually
Web Application Scans	
High	Quarterly or after significant ch
Medium	Semi-annually
Low	Annually

Remediation

Vulnerabilities discovered during scans must be remediated based on risk rating (see Table 2) and vulnerability severity identified by the scanning tool as per the table below.

TABLE 4: REMEDIATION TIMEFRAMES

Risk Rating (from Table 2)	Vulnerability Severity		
	Low or Below	Above Low to Below High	High or Above
High	At the discretion of the ISO/designated security representative	Action Plan in 2 Weeks, Resolved in 6 Months	Action Plan in 1 Week, Resolved in 1 Month
Medium	At the discretion of the ISO/designated security representative	Action Plan in 3 Weeks, Resolved in 1 year	Action Plan in 2 Weeks, Resolved in 6 Months
Low	At the discretion of the ISO/designated security representative	At the discretion of the ISO/designated security representative	Action Plan in 3 Weeks, Resolved 1 year

The IT Manager may review vulnerabilities to adjust the severity rating if necessary. Testing must be done to verify that remediation has been completed.

Individuals managing vulnerability scans are required to notify the ISO/designated security representative within 1 business day of scan completion for new vulnerabilities and at least monthly of un-remediated vulnerabilities on systems or applications that are running in production.

Detection Processes (DE.DP): Detection processes and procedures are maintainedand tested to ensure awareness of anomalous events.	**INCIDENT RESPONSE TRAINING** **Adirondack School Portraits shall:** **a. Provide incident response training to information system users consistent with assigned roles and responsibilities:** **i. Within 2 weeks of assuming an incident response role or responsibility.** **ii. When required by information system changes, and quarterly thereafter.** **b. Incorporate simulated events into incident response training to facilitate effective response by personnel in crisis situations.** **c. Employ automated mechanisms to provide a more thorough and realistic incident response training environment.** **1. INCIDENT RESPONSE TESTING** **Adirondack School Portraits shall:** **a. Coordinate incident response testing with BNL contacts responsible for related plans such as Business Continuity Plans, Contingency Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, and Occupant Emergency Plans.** **2. INCIDENT HANDLING** **Adirondack School Portraits shall:** **a. Implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.** **b. Coordinate incident handling activities with contingency planning activities.** **c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.** **3. INCIDENT MONITORING** **Adirondack School Portraits shall:** **a. Employ automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.** **4. INCIDENT REPORTING** **Adirondack School Portraits shall:** **a. Require personnel to report suspected security incidents to the incident response capability within 10 minutes of being aware of suspected incident.** **b. Report security incident information to IT Manager and Ownership** **5. INCIDENT RESPONSE PLAN** **Adirondack School Portraits shall:** **a. Develop an incident response plan that:** **i. Describes the structure of the incident response capability.** **ii. Provides a high-level approach for how the incident response capability fits into company's business operations.** **iii. Meets the unique requirements of company's business model, which relate to mission, size, structure, and functions.** **iv. Defines reportable incidents.**

	Detection Processes (DE.DP): Detection processes and procedures are maintainedand tested to ensure awareness of anomalous events.	v. **Provides metrics for measuring the incident response capability within the company.** vi. **Defines the resources and management support needed to effectively maintain and mature an incident response capability.** b. **Review the incident response plan Annually** c. **Update the incident response plan to address system changes or problems encountered during plan implementation, execution, or testing.** d. **Communicate incident response plan changes to Ownership** e. **Protect the incident response plan from unauthorized disclosure and modification.** **COMPLIANCE** **Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.**

Function	Category	Contractor Response
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	**IT Department shall:** **Develop a security plan for each information system that:** **Is consistent with the company's architecture.** **Defines explicitly the authorization boundary for the system.** **Describes the operational context of the information system in terms of missions and business processes.** **Provides the security categorization of the information system including supporting rationale.** **Describes the operational environment for the information system and relationships with or connections to other information systems.** **Provides an overview of the security requirements for the system.** **Identifies any relevant overlays, if applicable.** **Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions.** **Is reviewed and approved by the authorizing official or designated representative prior to plan implementation.** **Distribute copies of the security plan and communicate subsequent changes to the plan to authorized personnel and/or business units.** **Review the security plan for the information system at least annually.** **Update the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.** **Protect the security plan from unauthorized disclosure and modification.**

	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	**RULES OF BEHAVIOR** **IT Department shall:** **Establish, and make readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage.** **Receive a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.** **Review and update the rules of behavior.** **Require individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised and updated.** **INFORMATION SECURITY ARCHITECTURE** **IT Department shall:** **Develop information security architecture for the information system that will:** **Describe the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information.** **Describe how the information security architecture is integrated into and supports the enterprise architecture.** **Describe any information security assumptions and dependencies on external services.** **Review and update the information security architecture no less than annually, to reflect updates in the enterprise architecture.** **Ensure that planned information security architecture changes are reflected in the security plan, the security operations and procurements/acquisitions.** **DEFENSE-IN-DEPTH APPROACH** **IT Department shall:** **Design security architecture using a defense-in-depth approach that:** **Allocates security safeguards to the company's defined locations and architectural layers.** **Will ensure that the allocated security safeguards operate in a coordinated and mutually reinforcing manner.**

	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	**COMPUTER EMERGENCY RESPONSE** **A Computer Emergency Response Team (CCERT) shall be established. The CCERT shall be led by the IT Department Manager** **The CCERT shall consist of representatives from all departments.** **The CCERT shall communicate security information, guidelines for notification processes, identify potential security risks, and coordinate responses to thwart, mitigate, or eliminate security threats to IT resources.** **DEPARTMENTAL COMPUTER EMERGENCY RESPONSE** **Each department shall establish a Departmental Computer Emergency Response Team (DCERT) that is led by the IT Manager and has the responsibility for responding to and/or coordinating the response to security threats to IT resources within the department.** **Representatives from each DCERT shall also be active participants in CCERT.** **Upon the activation of a department's DCERT by the DISO, all DCERT representatives shall report directly to the DISO for the duration of the DCERT activation.** **Each department shall establish and implement Departmental Computer Emergency Response Procedures that consist of the following, at minimum:** **Creating an incident response policy and plan.** **Developing procedures for performing incident handling and reporting.** **Setting guidelines for communicating with outside parties regarding incidents.** **Selecting a team structure and staffing mode.** **Establishing relationships and lines of communication between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies.** **Determining what services the incident response team should provide.** **Staffing and training the incident response team.** **The DCERT shall inform the CCERT, as early as possible, of security threats to IT resources.** **Each department shall develop a notification process, to ensure**

	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	management notification within the department and to the CCERT, in response to IT security incidents. The CCERT and DCERTs have the responsibility to take necessary corrective action to remediate IT security incidents. Such action shall include all necessary steps to preserve evidence in order to facilitate the discovery, investigation, and prosecution of crimes against IT resources. Each department shall provide CCERT with contact information, including, without limitation, after-hours, for its primary and secondary CCERT and immediately notify CCERT of any changes to that information. Each department shall maintain current contact information for all personnel who are important for the response to security threats to IT resources and/or the remediation of IT security incidents. In instances where violation of any law may have occurred, proper notifications shall be made in accordance with IT policies. All necessary action shall be taken to preserve evidence and facilitate the administration of justice.
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	1.Network security personnel investigate alerts, to determine if an event or incident must be investigated. 2. If escalation is not required, the alert is closed. Events and incidents are investigated and triaged, based on the sensitivity of data and assets involved. 3. Incidents are categorized consistent with response plans. Post incident reviews are conducted to confirm an incident or event was classified appropriately.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	1. The IT Manager maintains an incident response plan that includes steps necessary to contain incidents. 2. The IT Manager receives and reviews monthly vulnerability reports to ensure all vulnerabilities are mitigated within expected

		timeframes
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	1. The IT Manger leads the incident response team through a lesson learned meeting after an incident response. 2. The IT Manager updates the incident response plan once all lessons learned are collected
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	The IT Manager ensures that the recovery plan is utilized during events that require a formal response.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	1. The IT Manager leads the incident response team through a lesson-learned meeting after an incident response. 2. The information security steering committee reviews the recovery strategies annually
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	1. Public relations are managed. The Ownership of Adirondack School Portraits is responsible for managing official messages during incidents. The Ownership of Adirondack School Portraits and other members of the executive team determine necessary steps for repairing reputational damage and communicate with external stakeholders.