Elwood Union Free School District
100 Kenneth Avenue
Greenlawn, New York 11740

Parents' Bill of Rights for Data Privacy and Security

The Elwood Union Free School District is committed to protecting the privacy and security of each and every student's data. Parents should be aware of the following rights they have concerning their child's data:

1. A student's personally identifiable information cannot be sold or released for any commercial or marketing purposes. A student's data cannot be shared with an unauthorized person.

2. Parents have the right to inspect and review the contents of their child's education record from their school. Parents' have the right to see the records within forty-five (45) days and dispute any inaccuracies.

3. The confidentiality of a student's personally identifiable information is protected by existing state and federal laws, and safeguards such as encryption, firewalls, and password protection, must be in place when data is stored or transferred. Third party contractors are required to employ technology, safeguards and practices that align with the National Institute of Standards and Technology Cybersecurity Framework.

4. A complete list of all student data elements collected by the State Education Department is available for public review at: https://www.nysed.gov/data-privacy-security/student-data-inventory, or by writing to the Office of Information & Reporting Services, New York State Education Department, 89 Washington Avenue, Room 863 EBA, Albany, NY 12234.

5. Parents have the right to file complaints about possible breaches of student data. Parents may submit a complaint regarding a potential breach by the District to Lorraine Dunkel, Assistant Superintendent for Business, 100 Kenneth Avenue, Greenlawn, New York 11740. The School District shall promptly acknowledge any complaints received and commence an investigation into the complaint, while taking the necessary precautions to protect personally identifiable information. The School District shall provide a response detailing its findings from the investigation no more than sixty (60) days after receipt of the complaint. Complaints pertaining to the State Education Department or one of its third party vendors may be submitted to NYSED at https://www.nysed.gov/data-privacy-security/parents-and-students-file-privacy-complaint, by mail to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Room 152 EB, Albany, NY 12234, or email to privacy@nysed.gov or by telephone at (518) 474-0937.

6. In the event of a data breach or unauthorized disclosure of students' personally identifiable information, third party contractors are required by law to notify in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.

7. If the District enters into a contract with a third party in which student, teacher, or principal data is shared with a third party, supplemental information for each such contract will be appended to this Parents' Bill of Rights.

8. Parents may access the State Education Department's Parents' Bill of Rights at: https://www.nysed.gov/data-privacy-security/bill-rights-data-privacy-and-security-parents-bill-rights

Acknowledged by: _____ Class Act Photographers 8/27/26

Organization Date

SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

As per the Agreement between the undersigned and the School District, this information must be completed by the Service Provider within ten (10) days of execution of the Agreement.

Name of Provider:	Class Act Photographers
Description of the purpose(s) for which Provider will receive/access PII:	Student information is provided to us 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 Provider will receive/access:	Check all that apply: ■ Student PII ☐ APPR Data
Contract Term:	Contract Start Date: 9/1/2026 Contract End Date: 6/30/2027
Subcontractor Written Agreement Requirement:	Provider 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) ☐ Provider will not utilize subcontractors. ■ Provider will utilize subcontractors.
Data Transition and Secure Destruction:	Upon expiration or termination of the Contract, Provider shall: • Securely transfer data to the School District, or a successor provider at the School District's option and written discretion, in a format agreed to by the parties. • Securely delete and destroy data.
Challenges to Data Accuracy:	Parents, teachers, or principals who seek to challenge the accuracy of PII will do so by contacting the School District. If a correction to data is deemed necessary, the School District will notify Provider. Provider agrees to facilitate such corrections within 21 days of receiving the School District'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. ☐ Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: Student Data and/or Principal or Teacher Data will be stored on-site and only accessible to personnel with qualified credential to protect data security and privacy risks are mitigated and protected using encryption
Encryption:	Data will be encrypted while in motion and at rest.

PROVIDER	
[Signature]	
[Printed Name]	John Repetti
[Title]	Manager
Date:	8/27/2026

Item	Details
• Provided the name of the data protection officer	All concerns related to data protection can be referred to: John Repetti - john@classactphoto.com
• Provided the main point of contact for the company, regarding technical support	Technical support contact is: John Repetti - john@classactphoto.com
• Provided the main point of contact for the company, regarding the service contract	Dan Repetti - dan@classactphoto.com
• Provided the process for how the district will be notified in the event of any changes to the points of contact	The staff at the district that monitors this contract will be notified via email of any changes
• Provided a rationale for the collection of each personal data element whether directly or in directly related to a person	Student information has been provided to us solely for student yearbook portraits, portrait package purchasing, student photo identification cards and for the purpose of communicating picture day details
• Provided the privacy notice for the product/service that clearly outlines the data retention period and means for destruction of data at the conclusion of the contract.	We further agree not to disclose any student information to a third party without the prior written/digital consent of the parent of the student or, if 18 years of age or older, the student. We agree not to retain student identification numbers assigned by the District after completing our services relative to student identification cards. All data will be wiped from our database at the expiration of the portrait services
• Trained staff who will be working with personal data on privacy best practices and have specific knowledge of education-based privacy requirements (e.g., NYS Part 121 NYCRR, NYS Ed. Law Sec. 2d, FERPA, IDEA)	Jacie Kim - jacie@classactphoto.com Jorge Rivera - jorge@classactphoto.com
• Trained staff who will be working with the personal data from our district on the components of the NIST Cybersecurity and Privacy Frameworks	John Repetti - john@classactphoto.com
• Administered safeguards to protect personal data of our students and staff	See Attachment 1 for Class Act Photographers NIST compliance
• Described subcontractors used to process personal data with details on how data is protected.	Class Act Photographers does not utilize any subcontractors that have access to PII

• Provided the locations of where personal data collected and processed on behalf of the district will be stored when at rest and how the transfer of data from one processing environment to another is protected.	The Class Act Photographers e-commerce 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 e-commerce 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.
• Provided a breach communication protocol that outlines how a notification of breach will be communicated and verified.	Class Act Photographers agrees to notify the district immediately upon the detection and/or notification of a data breach on any server housing district information at rest. Class Act Photographers agrees to cooperate with any specific compliance for the sending district in the event of a breach

Attachment 1

ATTACHMENT" 1."NISTCSFT_Process

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 Class Act Photographers 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 Class Act Photographers 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. j. Review accounts for compliance with account management requirements [entity defined frequency]. k. Employ automated mechanisms to support the management of information system accounts. l. Ensure that the information system automatically disables temporary and emergency accounts after usage. m. Ensure that the information system automatically disables inactive accounts after 30 days of inactivity
	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 service, our 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. As specific titles change from time to time, Class Act Photographers keeps a System Inventory outlining the products in use, and at what scope. We rely on our internal network infrastructure, for the 99.9+% uptime required for internet and system access necessary to successfully deliver our products to our customers.

Function	Category	Contractor Response
	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.	Class Act Photographers 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 externalpartners. Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, must beunderstood and managed. Governance and risk management processes will address cybersecurity risks.
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	1. RISK ASSESSMENT IT Department shall: a. Conduct an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits. b. Disseminate risk assessment results to Class Act Photographers business owners. c. Update the risk assessment quarterly or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system. 2. VULNERABILITY SCANNING IT Department shall: a. Scan for vulnerabilities in the information system and hosted applications real time to identity vulnerabilities potentially affecting the system/applications. b. Employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: Enumerating platforms, software flaws, and improper configurations. Formatting checklists and test procedures. Measuring vulnerability impact. c. Remediate legitimate vulnerabilities within one month in accordance

Function	Category	Contractor Response
		with an organizational assessment of risk. d. Share information obtained from the vulnerability scanning process and security control assessments with the owners of Class Act Photographers to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies). e. Employ vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned. f. Update the information system vulnerabilities scanned monthly, prior to a new scan, or when new vulnerabilities are identified and reported. g. Ensure that information systems implement privileged access authorization to all systems for selected vulnerability scanning. 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.
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**Information Statement** At Class Act Photographers 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 should be noted that an entity can never completely eliminate risk, but can take steps to manage risk. As per the Information Security Policy, any system or process that supports business functions must be appropriately managed for risk and undergo risk assessments as part of its life cycle. **Risk Management Process** The risk management process is iterative and should be followed throughout a system's or process's life cycle. **Frame Risk** The first step in managing risk is to: a. develop a strategy for conducting your risk assessment which considers assumptions, constraints, priorities, dependencies, tradeoffs and resources that will be used; and b. determine the risk tolerance, or the level of risk that is acceptable. For information security risk decisions that may

Function	Category	Contractor Response
		affect multiple entities, the lowest level of risk tolerance for those entities must prevail. It is important that entities recognize how fundamental this decision is to the risk management process. Risk tolerance is an executive-level decision and information technology (IT) staff should not be determining the risk tolerance for an entity. **Assess Risk** Assessing risk starts with identifying and classifying assets within scope. Risk is assessed by determining the threats and vulnerabilities to these assets, identifying the potential impact of each vulnerability being exploited, and determining the likelihood of occurrence. A list of potential threats and vulnerabilities needs to be developed, and may come from preexisting resources. It is important to note that the risk assessment process is comprehensive by intention, to assure due diligence, compliance, and proper documentation of security related controls and considerations. Designing security into systems requires an investment of time and resources. The extent of the risk assessment should be commensurate with the classification (information sensitivity and system criticality) of the system/process and the risks this system/process introduces into the overall environment. Types of information security risk assessments include, but are not limited to: • Enterprise Risk Assessments – Assesses risks to core agency assets, operational processes, and functions; • Physical Infrastructure Assets and Systems Risk Assessments – Identifies and assesses vulnerabilities and risks to core physical infrastructure assets and systems; • Project Security Risk Assessments (New Risks) – Identifies and assesses new risks to existing components introduced by new technology or service offerings; and • Change Request Risk Assessments – Assesses risk of change to ensure security is not compromised by the proposed change. **Respond to Risk** Once risk has been assessed, the entity must determine and implement the appropriate course of action. Options include: a. Risk Acceptance – This is a documented decision not to act on a given risk at a given time and place. It is not negligence or "inaction" and can be appropriate if the risk falls within the risk tolerance level. For example, entities may choose to accept the risk of an earthquake, based on a low likelihood in the Northeast of extensive damage and the high cost of controls. b. Risk Avoidance – These are specific actions taken to eliminate the activities or technologies that are the basis for the risk. This is appropriate when the identified risk exceeds the risk tolerance, even after controls have been applied (i.e., residual

Function	Category	Contractor Response
		risk). For example, if a connection between two networks includes unacceptable risks and the countermeasures are not practical, the entity may decide not to make the connection. c. Risk Mitigation/Reduction – These are specific actions taken to eliminate or reduce risk to an acceptable level. This is the most common approach and is appropriate where controls can reduce the identified risk. For example, to reduce the risk of network intrusion, an entity may choose to deploy a firewall. d. Risk Transfer/Sharing – These are specific actions taken to shift responsibility for the risk, in whole or in part, to a third party. This may be appropriate when it is more cost effective to transfer the risk, or when a third party is better suited to manage the risk. For example, an entity may transfer risk through legal disclaimers or by outsourcing to a vendor. **Monitor Risk** Class Act Photographers will monitor the effectiveness of its risk response measures, by verifying that the controls put in place are implemented correctly and operating as intended. This must occur annually, at a minimum. In addition, Class Act Photographers will have a process to alert it of significant changes in the factors it uses to assess its risk (e.g., assets, threats, controls, regulations, policies, risk tolerance). These changes may indicate a new assessment is needed.
	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.	This policy is applicable to all departments and users of IT resources and assets at Class Act Photographers. 1. ALLOCATION OF RESOURCES IT Department, in direct guidance and association with the information system owner shall: a. Determine information security requirements for the information system or information system service in mission/business process planning. b. Determine, document, and allocate the resources required to protect the information system or information system service as part of its capital planning and investment control process. c. Establish a discrete line item for information security in organizational programming and budgeting documentation. 2. SYSTEM DEVELOPMENT LIFE CYCLE IT Department, in direct guidance and association with the information system owner shall develop a contingency plan for the information system that: a. Manages the information system using the system development life cycle to ensure incorporation information security considerations. b. Defines and documents information security roles and responsibilities throughout the system development life cycle.

Function	Category	Contractor Response
		c. Identifies individuals having information security roles and responsibilities. d. Integrates the information security risk management process into system development life cycle activities. 3. ACQUISITION PROCESS IT shall ensure the acquisition process includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal, state, and local laws, Executive Orders, directives, policies, regulations, standards, guidelines, and mission and business needs: a. Security functional requirements. b. Security strength requirements. c. Security assurance requirements. d. Security-related documentation requirements. e. Requirements for protecting security-related documentation. f. Description of the information system development environment and environment in which the system is intended to operate. g. Acceptance criteria. SECURITY CONTROLS IT Department shall require the information system, system component, or information system service: a. Describe the functional properties of the security controls to be employed; security-relevant external system interfaces; high-level design, low-level design, source code or hardware schematics that meet the business requirements. b. Identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use. c. Employ only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within information systems. 5. INFORMATION SYSTEM DOCUMENTATION IT Department shall: a. Obtain administrator documentation for the information system, system component, or information system service that describes: i. Secure configuration, installation, and operation of the system, component, or service. ii. Effective use and maintenance of security functions/mechanisms. iii. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions. b. Obtain user documentation for the information system, system component, or information system service that describes i. User-accessible security functions/mechanisms and how to

Function	Category	Contractor Response
		effectively use those security functions/mechanisms. ii. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner. iii. User responsibilities in maintaining the security of the system, component, or service.
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.	Class Act Photographers IT Department shall: a. Identify and select the following types of information system accounts to support organizational missions and business functions: individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service. 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 by system owners 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 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. j. Review accounts for compliance with account management requirements monthly k. Employ automated mechanisms to support the management of information system accounts. l. Ensure that the information system automatically disables inactive accounts after 30 days of inactivity m. Ensure that the information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies appropriate IT personnel. 1. ACCESS ENFORCEMENT CAP IT Department shall: a. Ensure that the information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. 2. INFORMATION FLOW ENFORCEMENT IT Department shall: a. Ensure that the information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on applicable policy. 3. SEPARATION OF DUTIES

Function	Category	Contractor Response
		Class Act Photographers IT Department shall:Separate duties of individuals as necessary, to prevent malevolent activity without collusion.Document the separation of duties of individuals.Define information system access authorizations to support separation of duties.LEAST PRIVILEGEClass Act Photographers IT Department shall:Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.Authorize explicitly access to hardware and software controlling access to systems and filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists.Restrict privileged accounts on the information system to Class Act Photographers IT Department Manager..Ensure that the information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.UNSUCCESSFUL LOGON ATTEMPTSClass Act Photographers IT Department shall ensure that the information system:Enforces a limit of consecutive invalid logon attempts by a user during a daily 10 minute period.Locks the account/node automatically for 3 unsuccessful login attempts or until released by an administrator when the maximum number of unsuccessful attempts is exceeded.SYSTEM USE NOTIFICATIONClass Act Photographers IT Department shall ensure that the information system:Displays to users an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable state and federal laws, directives, policies, regulations, standards, and guidance and states informing that:Information system usage may be monitored, recorded, and subject to audit.Unauthorized use of the information system is prohibited and subject to criminal and civil penalties.Use of the information system indicates consent to monitoring and recording.There are not rights to privacy.Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system.

Function	Category	Contractor Response
		7. SESSION LOCK CAP T Department shall ensure that the information system: a. Prevent further access to the system by initiating a session lock after 30 days of inactivity or upon receiving a request from a user. b. Retain the session lock until the user reestablishes access using established identification and authentication procedures. c. Conceal, via the session lock, information previously visible on the display with a publicly viewable image. 8. SESSION TERMINATION Class Act Photographers IT Department shall: a. Ensure that the information system automatically terminates a user session after 10 minutes of inactivity. 9. PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION Class Act Photographers IT Department shall: a. Identify user actions that can be performed on the information system without identification or authentication consistent with organizational missions and business functions. b. Document and provide supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	This policy is applicable to all departments and users of IT resources and assets at Class Act Photographers 1. SECURITY AWARENESS TRAINING The Class Act Photographers IT Department shall: Schedule security awareness training as part of initial training for new users. b. Schedule security awareness training when required by information system changes and then annually thereafter. c. IT shall determine the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. The content shall: i. Include a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. ii. Address awareness of the need for operations security. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events. 2. SECURITY AWARENESS | INSIDER THREAT

Function	Category	Contractor Response
		IT Department shall:a. Include security awareness training on recognizing and reporting potential indicators of insider threat.ROLE-BASED SECURITY TRAININGClass Act Photographers IT Department shall:Provide role-based security training to personnel with assigned security roles and responsibilities:Before authorizing access to the information system or performing assigned duties.When required by information system changes and annually thereafter.PHYSICAL SECURITY CONTROLSIT Department shall: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, monitoring/surveillance equipment, and security guards (deployment and operating procedures).Identify personnel with specific roles and responsibilities associated with physical security controls requiring specialized training.SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIORIT Department shall:Provide training to its specified staff on how to recognize suspicious communications and anomalous behavior in organizational information systems.
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**Information StatementOrganizational Security**Information security requires both an information risk management function and an information technology security function. Depending on position at Class Act Photographers, an individual or group can serve in both roles or a separate individual or group can be designated for each role. It is recommended that these functions be performed by a high-level executive or a group that includes high level executives.Class Act Photographers will designate an individual to be responsible for the risk management function assuring that:risk-related considerations for information assets and individual information systems, including authorization decisions, are viewed as an enterprise with regard to the overall strategic goals and objectives of carrying out its core missions and business functions; andthe management of information assets and information system-related security risks is consistent, reflects the risk tolerance, and is considered along with other types of risks, to ensure mission/business success.

Function	Category	Contractor Response
		b. Although the technical information security function may be outsourced to third parties, Class Act Photographers retains overall responsibility for the security of the information that it owns. **Functional Responsibilities** **Executive management is responsible for:** 1. evaluating and accepting risk on behalf of Class Act Photographers. 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. promoting awareness of information security best practices through the regular dissemination of materials provided by the designated security representative; 6. implementing the process for determining information classification and categorization, based on industry recommended practices, organization directives, and legal and regulatory requirements, to determine the appropriate levels of protection for that information; 7. implementing the process for information asset identification, handling, use, transmission, and disposal based on information classification and categorization; 8. determining who will be assigned and serve as information owners while maintaining ultimate responsibility for the confidentiality, integrity, and availability of the data; 9. participating in the response to security incidents; 10. complying with notification requirements in the event of a breach of private information; 11. adhering to specific legal and regulatory requirements related to information security; 12. communicating legal and regulatory requirements to the designated security representative; and 13. 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. **The designated security representative is responsible for:** 1. maintaining familiarity with business functions and requirements; 2. maintaining an adequate level of current knowledge and proficiency in information security through annual Continuing Professional Education (CPE) credits directly related to information security; 3. assessing compliance with information security policies and legal and regulatory information security requirements; 4. evaluating and understanding information security risks and how to appropriately manage those risks; 5. representing and assuring security architecture considerations are addressed; 6. advising on security issues related to procurement of products and

Function	Category	Contractor Response
		services; 7. escalating security concerns that are not being adequately addressed according to the applicable reporting and escalation procedures; 8. disseminating threat information to appropriate parties; participating in the response to potential security incidents; 9. participating in the development of corporate policies and standards that considers BNL's needs; and 10. promoting information security awareness. **IT management is responsible for:** 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. providing training to appropriate technical staff on secure operations (e.g., secure coding, secure configuration); 6. fostering the participation of information security and technical staff in protecting information assets, and in identifying, selecting and implementing appropriate and cost-effective security controls and procedures; and implementing business continuity and disaster recovery plans. **The workforce is responsible for:** 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 information from unauthorized use or disclosure; 4. abiding by*Acceptable Use of Information Technology Resources* Policy 5. reporting suspected information security incidents or weaknesses to the appropriate manager and ISO/designated security representative. **The IT Department is responsible for:** 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; assessing compliance with security policies and standards; advising on secure system engineering; 6. providing incident response coordination and expertise;

Function	Category	Contractor Response
		monitoring networks for anomalies;monitoring external sources for indications of data breaches, defacements, etc.maintaining ongoing contact with security groups/associations and relevant authorities;providing timely notification of current threats and vulnerabilities; andproviding awareness materials and training resources.**Separation of Duties**To reduce the risk of accidental or deliberate system misuse, separation of duties and areas of responsibility must be implemented where appropriate.Whenever separation of duties is not technically feasible, other compensatory controls must be implemented, such as monitoring of activities, audit trails and management supervision.The audit and approval of security controls must always remain independent and segregated from the implementation of security controls.**Information Risk Management**Any system or process that supports business functions must be appropriately managed for information risk and undergo information risk assessments, at a minimum annually, as part of a secure system development life cycle.Information security risk assessments are required for new projects, implementations of new technologies, significant changes to the operating environment, or in response to the discovery of a significant vulnerability.Entities are responsible for selecting the risk assessment approach they will use based on their needs and any applicable laws, regulations, and policies.Risk assessment results, and the decisions made based on these results, must be documented.**Information Classification and Handling**All information, which is created, acquired or used in support of business activities, must only be used for its intended business purpose.All information assets must have an information owner established within the lines of business.Information must be properly managed from its creation, through authorized use, to proper disposal.All information must be classified on an ongoing basis based on its confidentiality, integrity and availability characteristics.An information asset must be classified based on the highest level necessitated by its individual data elements.If Class Act Photographers is unable to determine the confidentiality classification of information or the information is personal identifying information (PII)

Function	Category	Contractor Response
		the information must have a high confidentiality classification and, therefore, is subject to high confidentiality controls. g. Merging of information which creates a new information asset or situations that create the potential for merging (e.g., backup tape with multiple files) must be evaluated to determine if a new classification of the merged data is warranted. h. All reproductions of information in its entirety must carry the same confidentiality classification as the original. Partial reproductions need to be evaluated to determine if a new classification is warranted. i. Each classification has an approved set of baseline controls designed to protect these classifications and these controls must be followed. j. Class Act Photographers must communicate the requirements for secure handling of information to its workforce. k. A written or electronic inventory of all information assets must be maintained. l. PII must not be made available without appropriate safeguards approved by Class Act Photographers. m. For non-public information to be released outside of Class Act Photographers or shared between other entities, a process must be established that, at a minimum: 1. evaluates and documents the sensitivity of the information to be released or shared; 2. identifies the responsibilities of each party for protecting the information; 3. defines the minimum controls required to transmit and use the information; 4. records the measures that each party has in place to protect the information; 5. defines a method for compliance measurement; 6. provides a sign off procedure for each party to accept responsibilities; and 7. establishes a schedule and procedure for reviewing the controls. **IT Asset Management** a. All IT hardware and software assets must be assigned to a designated business unit or individual. b. Entities are required to maintain an inventory of hardware and software assets, including all system components (e.g., network address, machine name, software version) at a level of granularity deemed necessary for tracking and reporting. This inventory must be automated where technically feasible. c. Processes, including regular scanning, must be implemented to identify unauthorized hardware and/or software and notify appropriate staff when discovered. **Personnel Security** a. The workforce must receive general security awareness training, to include recognizing and reporting insider threats, within 30 days of hire. Additional training on specific security procedures, if required, must be completed before access is provided to specific Class Act Photographers sensitive information not covered in the general security training. All security

Function	Category	Contractor Response
		training must be reinforced at least annually and must be tracked by Class Act Photographers. b. Class Act Photographers will require its workforce to abide by the Policy, and an auditable process must be in place for users to acknowledge that they agree to abide by the policy's requirements. c. All job positions must be evaluated by IT Manager determine whether they require access to sensitive information and/or sensitive information technology assets. d. For those job positions requiring access to sensitive information and sensitive information technology assets, entities must conduct workforce suitability determinations, unless prohibited from doing so by law, regulation or contract. Depending on the risk level, suitability determinations may include, as appropriate and permissible, evaluation of criminal history record information or other reports from federal, state and private sources that maintain public and non-public records. The suitability determination must provide reasonable grounds for Class Act Photographers to conclude that an individual will likely be able to perform the required duties and responsibilities of the subject position without undue risk to Class Act Photographers. e. A process must be established within Class Act Photographers to repeat or review suitability determinations periodically and upon change of job duties or position. f. Entities are responsible for ensuring all issued property is returned prior to an employee's separation and accounts are disabled and access is removed immediately upon separation. **Cyber Incident Management** a. Class Act Photographers must have an incident response plan, consistent standards, to effectively respond to security incidents. b. All observed or suspected information security incidents or weaknesses are to be reported to appropriate management and the IT Department as quickly as possible. **Physical and Environmental Security** a. Information processing and storage facilities must have a defined security perimeter and appropriate security barriers and access controls. b. A periodic risk assessment must be performed for information processing and storage facilities to determine whether existing controls are operating correctly and if additional physical security measures are necessary. These measures must be implemented to mitigate the risks. c. Information technology equipment must be physically protected from security threats and environmental hazards. Special controls may also be necessary to protect supporting infrastructure and facilities such as electrical supply and cabling infrastructure. d. All information technology equipment and information media must be secured to prevent compromise of confidentiality, integrity, or availability in accordance with the classification of information contained therein. e. Visitors to information processing and storage facilities, including maintenance personnel, must be escorted at all times.

Function	Category	Contractor Response
		Account Management and Access Control a. All accounts must have an individual employee or group assigned to be responsible for account management. This may be a combination of the business unit and information technology (IT). b. Except as described in the Account Management/Access Control Standard, access to systems must be provided through the use of individually assigned unique identifiers, known as user-IDs. c. Associated with each user-ID is an authentication token (e.g., password, key fob, biometric) which must be used to authenticate the identity of the person or system requesting access. d. Automated techniques and controls must be implemented to lock a session and require authentication or re-authentication after a period of inactivity for any system where authentication is required. Information on the screen must be replaced with publicly viewable information (e.g., screen saver, blank screen, clock) during the session lock. e. Automated techniques and controls must be implemented to terminate a session after specific conditions are met as defined in the Account Management/Access Control Standard. f. Tokens must not be stored on paper, or in an electronic file, hand-held device or browser, unless they can be stored securely and the method of storing (e.g., password vault) has been approved by the ISO/designated security representative. g. Information owners are responsible for determining who should have access to protected resources within their jurisdiction, and what those access privileges should be (read, update, etc.). h. Access privileges will be granted in accordance with the user's job responsibilities and will be limited only to those necessary to accomplish assigned tasks in accordance with Class Act Photographers' missions and business functions (i.e., least privilege). i. Users of privileged accounts must use a separate, non-privileged account when performing normal business transactions (e.g., accessing the Internet, e-mail). j. Logon banners must be implemented on all systems where that feature exists to inform all users that the system is for business or other approved use consistent with policy, and that user activities may be monitored and the user should have no expectation of privacy. **Systems Security** a. Systems include but are not limited to servers, platforms, networks, communications, databases and software applications. 1. An individual or group must be assigned responsibility for maintenance and administration of any system deployed on behalf of Class Act Photographers. A list of assigned individuals or groups must be centrally maintained. 2. Security must be considered at system inception and documented as part of the decision to create or modify a system. 3. All systems must be developed, maintained and decommissioned in accordance with a secure system development lifecycle (SSDLC). 4. Each system must have a set of controls commensurate with the

Function	Category	Contractor Response
		classification of any data that is stored on or passes through the system. 5. All system clocks must synchronize to a centralized reference time source set to UTC (Coordinated Universal Time) which is itself synchronized to at least three synchronized time sources. 6. Environments and test plans must be established to validate the system works as intended prior to deployment in production. 7. Separation of environments (e.g., development, test, quality assurance, production) is required, either logically or physically, including separate environmental identifications (e.g., desktop background, labels). 8. Formal change control procedures for all systems must be developed, implemented and enforced. At a minimum, any change that may affect the production environment and/or production data must be included. a. <u>Databases and Software (including in-house or third party developed and commercial off the shelf (COTS):</u> 1. All software written for or deployed on systems must incorporate secure coding practices, to avoid the occurrence of common coding vulnerabilities and to be resilient to high-risk threats, before being deployed in production. 2. Once test data is developed, it must be protected and controlled for the life of the testing in accordance with the classification of the data. 3. Production data may be used for testing only if a business case is documented and approved in writing by the information owner and the following controls are applied: i. All security measures, including but not limited to access controls, system configurations and logging requirements for the production data are applied to the test environment and the data is deleted as soon as the testing is completed; or ii. sensitive data is masked or overwritten with fictional information. 4. Where technically feasible, development software and tools must not be maintained on production systems. 5. Where technically feasible, source code used to generate an application or software must not be stored on the production system running that application or software. 6. Scripts must be removed from production systems, except those required for the operation and maintenance of the system. 7. Privileged access to production systems by development staff must be restricted. 8. Migration processes must be documented and implemented to govern the transfer of software from the development environment up through the production environment.

Function	Category	Contractor Response
		Vulnerability Management a. All systems must be scanned for vulnerabilities before being installed in production and periodically thereafter. b. All systems are subject to periodic penetration testing. c. Penetration tests are required periodically for all critical environments/systems. d. Where Class Act Photographers has outsourced a system to another entity or a third party, vulnerability scanning/penetration testing must be coordinated. e. Scanning/testing and mitigation must be included in third party agreements. f. Appropriate action, such as patching or updating the system, must be taken to address discovered vulnerabilities. For any discovered vulnerability, a plan of action and milestones must be created, and updated accordingly, to document the planned remedial actions to mitigate vulnerabilities. g. Anyone authorized to perform vulnerability scanning/penetration testing must have a formal process defined, tested and followed at all times to minimize the possibility of disruption. **Operations Security** a. All systems and the physical facilities in which they are stored must have documented operating instructions, management processes and formal incident management procedures related to information security matters which define roles and responsibilities of affected individuals who operate or use them. b. System configurations must follow approved configuration standards. c. Advance planning and preparation must be performed to ensure the availability of adequate capacity and resources. System capacity must be monitored on an ongoing basis. d. Where the entity provides a server, application or network service to another entity, operational and management responsibilities must be coordinated by all impacted entities. e. Host based firewalls must be installed and enabled on all workstations to protect from threats and to restrict access to only that which is needed f. Controls must be implemented (e.g., anti-virus, software integrity checkers, web filtering) across systems where technically feasible to prevent and detect the introduction of malicious code or other threats. g. Controls must be implemented to disable automatic execution of content from removable media. h. Controls must be implemented to limit storage of information to authorized locations. i. Controls must be in place to allow only approved software to run on a system and prevent execution of all other software. j. All systems must be maintained at a vendor-supported level to ensure accuracy and integrity. k. All security patches must be reviewed, evaluated and appropriately applied in a timely manner. This process must be automated, where technically possible. l. Systems which can no longer be supported or patched to current

Function	Category	Contractor Response
		versions must be removed. m. Systems and applications must be monitored and analyzed to detect deviation from the access control requirements outlined in this policy and theSecurity Logging Standard, and record events to provide evidence and to reconstruct lost or damaged data. n. Audit logs recording exceptions and other security-relevant events must be produced, protected and kept consistent with record retention schedules and requirements. o. Monitoring systems must be deployed (e.g., intrusion detection/prevention systems) at strategic locations to monitor inbound, outbound and internal network traffic. p. Monitoring systems must be configured to alert incident response personnel to indications of compromise or potential compromise. q. Contingency plans (e.g., business continuity plans, disaster recovery plans, continuity of operations plans) must be established and tested regularly. 1. An evaluation of the criticality of systems used in information processing (including but not limited to software and operating systems, firewalls, switches, routers and other communication equipment). 2. Recovery Time Objectives (RTO)/Recovery Point Objectives (RPO) for all critical systems. r. Backup copies of entity information, software, and system images must be taken regularly in accordance with the entity's defined requirements. s. Backups and restoration must be tested regularly. Separation of duties must be applied to these functions. t. Procedures must be established to maintain information security during an adverse event. For those controls that cannot be maintained, compensatory controls must be in place.
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	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 CAP 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

Function	Category	Contractor Response
		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 CAP IT Department shall: a. Analyze changes to the information system to determine potential security impacts prior to change implementation. 4. ACCESS RESTRICTIONS FOR CHANGE IT Department shall: a. Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system. 5. CONFIGURATION SETTINGS IT Department shall: a. Establish and document configuration settings for information technology products employed within the information system. b. Implement the configuration settings. c. Monitor and control changes to the configuration settings in accordance with policies and procedures. 6. LEAST FUNCTIONALITY Class Act Photographers IT Department shall: a. Configure the information system to provide only essential capabilities. b. Review the information system quarterly to identify unnecessary and/or non-secure functions, ports, protocols, and services. c. Disable functions, ports, protocols, and services within the information system deemed to be unnecessary and/or non-secure. d. Prevent program execution in accordance with policies regarding software program usage and restrictions and rules authorizing the terms and conditions of software program usage. e. Identify software programs not authorized to execute on information systems. f. Employ an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system. g. Review and update the list of unauthorized software programs annually. 7. INFORMATION SYSTEM COMPONENT INVENTORY Class Act Photographers IT Department shall: a. Develop and document an inventory of information system components that: i. Reflects the current information system accurately. ii. Includes all components within the authorization boundary of the information system.

Function	Category	Contractor Response
		iii. Is at the level of granularity deemed necessary for tracking and reporting. iv. Includes information deemed necessary to achieve effective information system component accountability. b. Review and update the information system component inventory annually. c. Update the inventory of information system components as an integral part of component installations, removals, and information system updates. d. Employ automated mechanisms quarterly to detect the presence of unauthorized hardware, software, and firmware components within the information system. e. Take the following actions when unauthorized components are detected: i. Disable network access by such components, or ii. Isolate the components and notifies the Chief Information Officer and system owner. f. Verify that all components within the authorization boundary of the information system are not duplicated in other information system component inventories. 8. CONFIGURATION MANAGEMENT PLAN IT shall develop, document, and implement a configuration management plan for the information system that: a. Addresses roles, responsibilities, and configuration management processes and procedures. b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items. c. Defines the configuration items for the information system and places the configuration items under configuration management. d. Protects the configuration management plan from unauthorized disclosure and modification. 9. SOFTWARE USAGE RESTRICTIONS Class Act Photographers IT Department shall: a. Use software and associated documentation in accordance with contract agreements and copyright laws. b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution. c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	CONTROLLED MAINTENANCE Class Act Photographers 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 and/or requirements conducted by local IT and/or outsourced IT entities. b. Approve and monitor all maintenance activities, whether performed

Function	Category	Contractor Response
		on site or remotely and whether the equipment is serviced on site or removed to another location. c. Require that system owners explicitly approve the removal of the information system or system components from facilities for off-site maintenance or repairs. d. Sanitize equipment to remove all information from associated media prior to removal from Class Act Photographers facilities for off-site maintenance or repairs. e. Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions. f. Include IT and system owner's defined maintenance-related information in maintenance records. g. For those components not directly associated with information processing such as scanners, copiers, and printers, maintenance records must include date and time of maintenance, entity performing the maintenance, maintenance performed, components replaced or removed including identification/serial numbers as applicable. 1. MAINTENANCE TOOLS Class Act Photographers 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. 2. NONLOCAL MAINTENANCE Class Act Photographers IT Department shall: a. Approve and monitor non-local maintenance and diagnostic activities. b. Allow the use of nonlocal 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 nonlocal maintenance and diagnostic sessions. d. Maintain records for nonlocal maintenance and diagnostic activities. e. Terminate session and network connections when nonlocal maintenance is completed. f. Document in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections. 3. MAINTENANCE PERSONNEL Class Act Photographers 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.

Function	Category	Contractor Response
		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. 4. TIMELY MAINTENANCE Class Act Photographers IT Department shall: 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 ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	1. MEDIA ACCESS: Class Act Photographers 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 Class Act Photographers 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 Class Act Photographers 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 Class Act Photographers 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

Function	Category	Contractor Response
		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 Class Act Photographers 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 Class Act Photographers 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 Class Act Photographers IT Department shall: a. Monitor the information system to detect: i. Attacks and indicators of potential attacks. 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.

Function	Category	Contractor Response
		SECURITY ALERTS, ADVISORIES, AND DIRECTIVES Class Act Photographers 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 Class Act Photographers IT Department shall: a. Employ spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages. 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 Class Act Photographers 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. 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** The 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. **Type** | **Description** **External Infrastructure Scan** | Scans of the perimeter of networksor any

Function	Category	Contractor Response

	infrastructure to identify potential vulnerabil infrastructure.
Internal Infrastructure Scan	Scans of IT infrastructure on protected netw infrastructure to identify potentialvulnerabil
"Lite" Web Application Scan	Cursory unauthenticated scans of externally applications to identify securityvulnerabil
In-depth Web Application Scan	When implemented, authenticated in-depth toidentify security vulnerabilities.
Application Source Code Analysis	Scans of application source code run during de problems in the code that couldcause

Scanning

Class Act Photographers IT Manager is responsible for confirming that vulnerability scans are conducted. 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.

Function	Category	Contractor Response
		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. 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.

Function	Category	Contractor Response
		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 internetfacing)	System that is publi internet
High	Medium	High	High
Medium	Low	Medium	High
Low	Low	Low	Medium

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

<table>
<tr><th>Function</th><th>Category</th><th>Contractor Response</th></tr>
<tr><td></td><td></td><td>
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>
<tr><th colspan="4">TABLE 4: REMEDIATION TIMEFRAMES</th></tr>
<tr><td rowspan="2">Risk Rating (from Table 2)</td><td colspan="3">Vulnerability Severity</td></tr>
<tr><td>Low or Below</td><td>Above Low to Below High</td><td>High or Above</td></tr>
<tr><td>High</td><td>At the discretion of the ISO/designated securityrepresentative</td><td>Action Plan in 2 Weeks,Resolved in 6 Months</td><td>Action Plan in 1 Week, R</td></tr>
<tr><td>Medium</td><td>At the discretion of the ISO/designated securityrepresentative</td><td>Action Plan in 3 Weeks,Resolved in 1 year</td><td>Action Plan in 2 Weeks,</td></tr>
<tr><td>Low</td><td>At the discretion of the ISO/designated securityrepresentative</td><td>At the discretion of the ISO/designated securityrepresentative</td><td>Action Plan in 3 Weeks,</td></tr>
</table>
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.
</td></tr>
<tr><td></td><td>Detection Processes (DE.DP):
Detection processes and procedures are maintained and tested to ensure awareness of</td><td>
INCIDENT RESPONSE TRAINING
Class Act Photographers 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.
</td></tr>
</table>

Function	Category	Contractor Response
	anomalous events.	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 Class Act Photographers shall: a. Coordinate incident response testing with Class Act Photographers 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 Class Act Photographers 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 Class Act Photographers 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 Class Act Photographers 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 Class Act Photographers 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 Class Act Photographers iii. Meets the unique requirements of Class Act Photographers, which relate to mission, size, structure, and functions. iv. Defines reportable incidents. v. Provides metrics for measuring the incident response capability within Class Act Photographers vi. Defines the resources and management support needed to effectively maintain and mature an incident response capability. 6. Review the incident response plan Annually c. Update the incident response plan to address system changes or problems encountered during plan implementation, execution, or

Function	Category	Contractor Response
		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.
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 Class Act Photographers' 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.

Function	Category	Contractor Response
		Protect the security plan from unauthorized disclosure and modification. 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 Class Act Photographers's defined locations and architectural layers. Will ensure that the allocated security safeguards operate in a coordinated and mutually reinforcing manner.

Function	Category	Contractor Response
	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 management notification within the department and to the CCERT, in response to IT security incidents.

Function	Category	Contractor Response
		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. Each department shall provide its primary and secondary CCERT representatives with adequate portable communication devices (e.g., cell phone and pager). 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 is maintains and incident response plan that includes steps necessary to mitigate incidents. 3. 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.

Function	Category	Contractor Response
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.	1. Public relations are managed. The Ownership of Class Act Photographers is responsible for managing official messages during incidents. 2. The Ownership of Class Act Photographers and other members of the executive team determine necessary steps for repairing reputational damage and communicate with external stakeholders.