shutterstock

EFFECTIVE DATE
January 30, 2023
(Policy Effective Date)

Information Security Policy

1. **Information security.** Shutterstock receives, uses, and generates Personal Information and Sensitive Personal Information about our employees, contributors, customers, contractors, and others, as well as proprietary information about our business and financial affairs (collectively, "Protected Information"). Shutterstock collects, processes, stores and transmits information in many forms including electronic, physical, and verbal. The Shutterstock Information Security Program (the "Information Security Program" or "Program") is designed to ensure the safeguarding of all information in Shutterstock's possession in accordance with applicable law by establishing policies, practices, and procedures, and implementing technical, administrative, and physical measures, to protect it.

    1.1 This Policy looks to minimize the risk of damage by reducing the potential impact from security events through the establishment and maintenance of security and confidentiality of Shutterstock assets. This is accomplished by enforcing the following concepts:

        1.1.1 **Confidentiality**. Confidentiality is the security principle that controls access to information. It is designed to protect information from being accessed by unauthorized users while ensuring the right users can access it. Confidentiality can be compromised in several ways. Commonly encountered threats to information confidentiality include hackers, masquerading, networks, malicious software, and social engineering.

        1.1.2 **Integrity**. Integrity is the assurance that information remains trustworthy and accurate. Data must not be changed in transit, and steps must be taken to protect data from modification or deletion by unauthorized users. One type of security attack is to intercept some important data and make changes to it before sending it on to the intended receiver. Methods used to establish integrity controls include separation of duties and access based on least privilege.

        1.1.3 **Availability**. Availability guarantees reliable access to the information; systems work promptly, and service is not denied to authorized users. Threats to availability include denial of service incidents and a loss of data processing capabilities as a result of natural disaster or human actions.

    1.2 **Scope.** The Information Security Program establishes rules and procedures for protecting both the information in Shutterstock's possession and the information systems used to Process or access such information. The Program includes this document, as well as various related policies and procedures setting forth more detailed rules for specific areas of concern as they may be adopted from time to time (the "Policies and Procedures"). This policy applies to all assets, information, information systems, networks, applications, locations and users of Shutterstock or supplied under contact to it. This policy establishes rules and procedures for protecting both information in Shutterstock's possession and the information systems used to process and access such information

    1.3 **Delegation**. Shutterstock's Chief Information Security Officer and Privacy Officer are responsible for implementing the Information Security Program and is authorized to delegate tasks and responsibilities as appropriate to achieve its objectives.

2. Definitions

2.1 **Personal Information** means any information relating to an identified or identifiable natural person, even if an individual's name is not specifically mentioned.

2.2 **Sensitive Personal Information** means information that is defined as sensitive under state, federal, provincial, national or international law.

2.2.1 In the United States, this data includes, for example, social security number; driver's license number or other state ID number; bank, credit, or debit card account numbers; other financial account numbers; passwords or unique identifiers used to access personal financial information; medical or health information; the maiden name of the person's mother; date of birth; employer-assigned number or other identifier; passport number; digital signatures; fingerprints or other biometric data; certain online login information; and precise geographic location information.

2.2.2 In the European Union and United Kingdom, this data includes racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data for the purpose of uniquely identifying a natural person; health; and sexual life or orientation.

2.2.3 In Canada, this data includes, for example, any information, recorded in any form, about an identified individual or an individual whose identity may be inferred or determined from such information, other than business contact information (e.g. name, title, business address). This would also include any information relating to a person's health.

2.2.4 In Brazil, this data includes personal data on racial and ethnic origin, religious belief, political opinion, affiliation to a trade union or organization of a religious, philosophical or political character, data referring to health or sexual life, genetic or biometric data, when linked to a natural person.

2.3 **Proprietary Information** means (a) general and technical information concerning Shutterstock's current and prospective products and services, including computer programs, systems, techniques, machines, methodology, product data and specifications, formulae, compositions, diagrams, flow charts, drawings, test results, know-how, processes, inventions, research projects and product development; (b) business information concerning the conduct of Shutterstock's businesses, including customer lists and customer information, pricing data, cost information, profits, sales information, accounting and unpublished financial information, business plans, marketing, public relations, production or merchandising systems, plans, techniques and/or methods, purchasing, supplier lists and supplier information and advertising strategies; (c) any and all versions of Shutterstock's computer software (including source code and object code) and computer graphics, hardware, firmware and documentation; (d) information concerning Shutterstock's employees, including their salaries, strengths, weaknesses and skills; (e) information regarding potential merger and acquisition targets, strategic partners, and the like; and (f) information submitted by Shutterstock's clients, customers, suppliers, employees, consultants or co-venturers with Shutterstock for study, evaluation or use.

2.4 **Protected Information** means all nonpublic information in Shutterstock's possession, including Personal Information, Sensitive Personal Information, Proprietary Information, and information about corporate entities that are not specifically protected by the laws and regulations regarding personal data or privacy.

2.5 **Process** means to perform any operation(s) (automated or manual) on Personal Information and Proprietary Information, such as collection, recording, organization, storage, adaptation, alteration, retrieval, combination, consultation, use, disclosure by transmission, dissemination, blocking, erasure, or destruction. Processing may use equipment or facilities of Shutterstock, Service Providers, or a Third Party.

2.6 **Service Provider** means any individual, entity (including vendors and marketing and joint venture partners), or agent of an entity, that receives, maintains, Processes, or otherwise is

permitted to access Protected Information through its provision of services to Shutterstock (including its branch offices) or its customers.

2.7 **Third Party** means any unaffiliated entity or any individual not an employee of Shutterstock and not a Service Provider.

3. **Organization of Information Security**

3.1 **Responsibility for information security.** Information security is the responsibility of all employees at Shutterstock. Additionally, the responsibility for implementation and oversight of the Information Security Program will be driven by the Chief Information Security Officer, in consultation with the Privacy Officer.

3.2 **Role of Chief Information Security Officer and Cybersecurity & Risk Management Department**. Shutterstock shall appoint a Chief Information Security Officer, who shall exercise the following duties (directly, or by appropriate delegation of responsibility) with independent judgment and in coordination with the Privacy Officer

3.2.1 Drive security accountability throughout the organization by developing systems, process and procedures to facilitate implementation of and compliance with provisions of this Program;

3.2.2 Conduct a security risk assessment periodically or as appropriate and, in light of the results, work with the Privacy Officer to revise the systems and procedures related to information security as necessary to achieve the purposes of this Program;

3.2.3 Chair a Security Steering Committee whose purpose is to improve the posture of cybersecurity, coordinate corporate security initiatives at the executive level and enable the organization to optimize spending, manage infrastructure and minimize security risks.

3.2.4 Establish guidelines as appropriate for Shutterstock personnel and Service Providers with authorized access to and responsibilities for information systems;

3.2.5 Maintain security monitoring tools and review and analyze security alerts. Communicate results and necessary actions to appropriate technology and business owners.

3.2.6 Identify and review key controls, systems, and procedures; maintain up-to-date security and patching; investigate and respond to security incidents in accordance with a written incident response plan, as needed;

3.2.7 Regularly test key controls and procedures, including conducting periodic penetration testing of Shutterstock networks and systems.

3.2.8 Monitor laws (in collaboration with Legal), rules, and industry standards with respect to information security and data privacy and, in consultation with the Privacy Officer, revise this Program as appropriate to reflect relevant changes in laws, rules, and industry best practices;

3.2.9 Work with Shutterstock personnel to ensure that each system used to Process Personal Information and Proprietary Information is protected by administrative, technical, and physical safeguards that are appropriate to the size, complexity, nature and scope of the system and the sensitivity classification of any Personal Information or Proprietary Information being Processed.

3.2.10 Work with appropriate Shutterstock personnel to establish systems and procedures necessary to ensure that:

3.2.10.1 New information systems and new elements of existing systems are compliant with the provisions of this Program;

3.2.10.2 All Shutterstock personnel and Service Providers understand and comply with the provisions of this Program related to information security;

3.2.10.3 Requests for access to Protected Information are granted on a need-to-know basis; and

3.2.10.4 Significant non-compliance events and security incidents are identified, contained, investigated, and responded to as required by this Program and applicable law.

3.2.11 Ensure physical security measures, policies and procedures are in place that: (i) are designed to deny unauthorized access to facilities, equipment, and resources; (ii) protect personnel and property from damage and harm; (iii) protect paper records containing Personal Information from unauthorized access and other physical and environmental threats; and (iv) ensure that records containing Personal Information that are no longer required for operational purposes are securely stored offsite and/or securely destroyed in accordance with the Records Management Policy.

3.2.12 Work with appropriate Shutterstock personnel to (i) circulate this Program; (ii) make presentations to Shutterstock personnel; (iii) develop training, guidance, and educational materials about Protected Information privacy and data protection issues in general and the policies and procedures set forth in this Program in particular; and (iv) promote awareness of and enhance compliance with this Program throughout Shutterstock;

3.2.13 Provide annual reports and updates as appropriate to Senior Management regarding Personal Information privacy and Security threats, risks and issues and the Company's compliance to the Program policies and procedures.

3.3 **Role of Privacy Officer**. Shutterstock's management shall appoint a Privacy Officer, who shall exercise the following duties (directly or by appropriate delegation of responsibility) with independent judgment and in coordination with the Chief Information Security Officer:

3.3.1 Implement the policies and procedures set forth in this Program to achieve compliance with Shutterstock's data protection obligations;

3.3.2 Regularly review this Program to ensure compliance with applicable law, regulatory and self-regulatory obligations, and codes with respect to privacy and data security, and changing private sector practices;

3.3.3 Work with appropriate Shutterstock personnel and counsel to develop and implement compliant privacy policies;

3.3.4 Work with appropriate Shutterstock personnel to ensure compliance with applicable law requiring notification of Data Subjects and/or Data Protection Authorities in the event of an information security incident involving Personal Information;

3.3.5 Ensure that Authorized Users and other relevant Shutterstock personnel have executed confidentiality agreements, in the form approved by Shutterstock, that obligate them to safeguard Protected Information;

3.3.6 Work with the Chief Information Security Officer, as set forth in section 3.2 above; and

3.3.7 Undertake any other duties that may be identified from time to time by Senior Management.

3.4 Conflicting duties and areas of responsibility must be segregated either within departments or across departments to reduce opportunities for unauthorized or unintentional modification or misuse of Shutterstock assets

3.5 Information security must be addressed in project management, regardless of the type of the project

4. **Risk Management**

4.1 **Assessing security risks**. The Chief Information Security Officer will conduct periodic (but no less than annual) assessments of internal and external security risks to Protected

Information and to systems used to Process or access that information. Such assessments also will be conducted in the event of material changes in law, industry practices, or relevant Shutterstock activities.

4.2 **Responding to identified risks**. The Chief Information Security Officer will report any material risks identified in the course of assessing security risks to Shutterstock's senior management. The Chief Information Security Officer will work with the Privacy Officer and senior management to develop and implement policies, practices, and procedures to mitigate such risks.

4.3 The risk treatment approach will vary based on the type of activity, may change over time, and may include the following:

4.3.1 Risk Reduction: Implement safeguards to reduce risks;

4.3.2 Risk Acceptance: Recognize and accept risks without additional steps;

4.3.3 Risk Avoidance: Deem the activity too risky, even when combined with other treatment options;

4.3.4 Risk Sharing: Sharing the economic aspect of risks with Third Parties

5. **Information and Asset Management**

5.1 **Collection limitation**. Shutterstock will limit collection of Protected Information to that which is necessary to accomplish legitimate business, and which complies with applicable laws, rules of professional conduct, and Shutterstock policies.

5.2 **Inventory of Shutterstock information systems**. Shutterstock will create, maintain, and as appropriate update a firm-wide inventory of information systems, devices, software platforms, and applications used to Process or access Protected Information. The asset inventory must include enough information about the asset to identify the following:

5.2.1 Asset Owner / Responsible party for maintaining the Asset;

5.2.2 Location (physical or virtual);

5.2.3 Intended use;

5.2.4 Classification (both by regulatory requirement, if any, and information housed or processes);

5.2.5 Connection to or dependence on other assets;

5.2.6 Maintenance window;

5.3 **Responsibility for information systems used to Process or access Protected Information**. An Asset Owner (Responsible party) shall be responsible for each information system used to Process or access Protected Information who will have primary responsibility for ensuring that each system maintain technical practices and procedures to safeguard such information and systems in compliance with the standards developed by the Chief Information Security Officer and Security Steering Committee.

5.4 **Acceptable use of information systems**. The Privacy Officer and Chief Information Security Officer will collaborate to develop, implement, and as appropriate update Shutterstock's Acceptable Use Policy.

5.5 **Information retention policy**. Shutterstock will securely dispose of Assets when no longer required by the company so that Protected Information is securely destroyed when no longer needed for a legitimate business purpose or to comply with applicable law and the Records Management Policy. The secure disposal of assets must be documented by formal procedures or evidence.

5.6 **Information classification and inventory**. The company will maintain and manage a firm-wide inventory of all Protected Information, including relevant classifications for legal

compliance, value, and sensitivity. Shutterstock's policy is to safeguard all information in its possession in accordance with this Information Security Program.

5.7 All employees and Third-Party users of Shutterstock information assets must return all of Shutterstock's assets in their possession upon termination of their employment or engagement.

5.8 Procedures must be implemented for the management of removable media Assets in accordance with Shutterstock's Information Classification Schema. Any physical transfer of removable media Assets must be protected against unauthorized access, misuse or corruption.

6. **Human Resources Security**

6.1 **Practices and procedures**. Shutterstock shall implement practices, procedures, and training designed to ensure that personnel are aware of such established policies, practices and procedures and comply with their obligations to safeguard Protected Information.

6.2 **New personnel**. All Shutterstock personnel shall be subject to background and reference checks, as appropriate and where permitted by applicable law, before hire. Security responsibilities shall be explicitly conveyed to all new Shutterstock personnel, and new Shutterstock personnel shall be required to acknowledge in writing their receipt, understanding, and willingness to accept these responsibilities. Among other things, the Privacy Officer will ensure that relevant personnel have executed confidentiality agreements, in the form approved by Shutterstock, that obligate them to safeguard Personal Information.

6.3 **Ongoing education and training**. Shutterstock shall employ a training and awareness program to educate employees about information security procedures and the safeguarding of Protected Information. Employees shall be trained at time of hire. All employees will receive ongoing training on an annual basis. Software developers will receive annual training on secure coding techniques and development teams will comply with the Shutterstock Secure Coding Policy. Shutterstock will maintain training materials and policies that are easily accessible for employees to reference. The company will maintain records of trainings delivered and employees shall acknowledge receipt and understanding.

6.4 Information security procedures with respect to contractors shall be addressed in the written consulting agreement between Shutterstock and the contractor's employer.

6.5 **Disciplinary procedure**. Any person who deliberately Processes or attempts to Process information without authorization or in a manner that violates security policies and/or procedures shall be subject to appropriate disciplinary action, up to and including termination of employment.

6.6 **Termination or change of employment.** Shutterstock will maintain procedures to manage personnel separation that ensure the return or other appropriate disposition of all Shutterstock information assets, including Protected Information, information processing equipment, or other Shutterstock property used to Process or access Protected Information. Shutterstock will maintain procedures to ensure that access rights are promptly removed or modified upon an employee's separation or change of responsibilities.

7. **Physical and Environmental Security**

7.1 **Secure areas**. Each of Shutterstock's offices and data processing facilities shall maintain defined security perimeters, appropriate physical and electronic security barriers, and entry practices and procedures designed to protect Protected Information from unauthorized access, alteration, and misuse.

7.1.1 Barriers can include doors and locks, key card entry, manned entry and reception points, cameras, gates and fences, and/or fire doors and alarms.

7.1.2 Processes can include requiring wearing or carrying some form of visible ID/key card; maintaining a visitor log with time in/out, date and Shutterstock sponsor; periodic review of key card access/entry/exit; and/or periodic review of camera footage.

7.2 **Equipment security.** Shutterstock will adopt and maintain practices and procedures designed to protect equipment used to Process or access Protected Information, including equipment used off-site or remotely.

7.2.1 Shutterstock information must be removed or securely overwritten prior to disposal or reuse of equipment.

7.2.2 Workstations containing or used to access Shutterstock information or assets must be secured when not in use.

7.2.3 Information stored or accessible via laptops and other mobile devices must be secured.

7.2.4 Networking equipment, power and cabling must be protected from unauthorized access and physical or environmental harm.

7.2.5 Equipment and assets must be maintained to ensure its continued availability and integrity.

7.3 Security for paper records. Departments keeping or maintaining paper records containing Protected Information must ensure they are stored securely (e.g. in locked filing cabinets) allowing access only to those with a legitimate business need.

8. **Service Provider Management**

8.1 Shutterstock shall implement and maintain policies and procedures for selecting and supervising Service Providers that may Process or have access to Protected Information. Such practices and procedures will provide, without limitation, as follows:

8.1.1 **Vetting**. Shutterstock will engage reputable Service Providers who will screen employees and/or agents likely to Process or have access to Protected Information.

8.1.2 Shutterstock will take reasonable steps to confirm by contractual representations and/or audits that any Service Provider that will have access to Protected Information has and maintains the ability to comply with all relevant federal, state, and national data security laws, such as the Gramm-Leach-Bliley Act (including its implementing rules and guidelines, as well as all state analogues) (collectively, "GLBA") , the Massachusetts data security requirements contained in 201 CMR 17.00 et seq., implementing the provisions of M.G.L. c. 93H (the "Massachusetts Security Regulation"), the California Consumer Protection Act ("CCPA"), the Personal Information Protection of Electronic Documents Act ("PIPEDA") in Ontario, and An Act Respecting the Protection of Personal Information in the Private Sector ("PPIPS") in Quebec, Personal Data Protection Act ("PDPA") in Singapore, and other national personal data protection laws.

8.1.3 **Written undertakings**. Shutterstock will obtain written undertakings from Service Providers that will have access to Protected Information that they will safeguard such information as required by law and in accordance with recognized standards for information security.

8.1.4 **Personal Information**. Shutterstock will obtain written confirmation from Service Providers that will Process or have access to Personal Information that they will implement information security safeguards that are at least as stringent as those required to be applied to Personal Information under GLBA, the Massachusetts Security Regulation, PIPEDA and PPIPS, CCPA, PDPA, and other federal, state, and national personal data protection laws as applicable. Within the scope of application of EU General Data Protection Regulation and UK Data Protection Act (2018), Shutterstock will ensure its compliance with the requirements for the processing of Personal Information by a processor.

8.1.5 **Service Provider responsibilities**. Supervisors should explain Shutterstock's information security requirements to any Service Provider working on-site or having remote access to Protected Information.

8.1.6 **Monitoring**. The Shutterstock owner of the relationship is responsible for ensuring the Service Provider complies with all relevant information security policies and procedures as required, including following established information security procedures for ensuring that Service Provider access rights are reasonable and appropriate. Such procedures shall include regular monitoring, review, auditing, and any other appropriate supervision of Service Providers to ensure Service Providers are complying with relevant privacy and data security laws and ensuring that any information security incident is appropriately reported to the Chief Information Security Officer for management.

8.1.7 **Return or destroy**. At the conclusion of a Service Provider's evaluation of any Protected Information, termination of any contract between Shutterstock and the Service Provider for services involving access to such information, or on Shutterstock's demand, a Service Provider shall be required to immediately return to Shutterstock or destroy any and all such information. The Service Provider also shall be required to promptly certify to Shutterstock that it has purged its records and/or files of such information.

9. **Communications and Operations Management**

9.1 Shutterstock will implement commercially reasonable practices and procedures, including baseline system configurations designed, as appropriate, to:

9.1.1 Safeguard Protected Information in networks; Sensitive Personal Information and other information at the highest level of classification must be prevented from unencrypted transmission outside Shutterstock (including to vendors and partners);

9.1.2 Protect documents and computer media containing Protected Information from unauthorized disclosure, modification, removal, and destruction;

9.1.3 Prevent the introduction of, detect the presence of, and remove malicious code, including up-to-date firewall protection, virus definitions, malware protections, and application and operating system security patches as feasible and appropriate.

9.1.4 Document incident management and response plans for handling of errors and other unexpected conditions;

9.1.5 Monitor, detect, and log actions that could affect or be relevant to the confidentiality, integrity and availability of Shutterstock information;

9.1.6 Separate different operating environments (Dev, Test, QA, Prod) to reduce the risk of unauthorized access or change;

9.1.7 Manage and control networks used by Shutterstock in order to secure Protected Information in systems and applications.

9.1.8 Ensure that Shutterstock engages in appropriate backup practices and that essential Protected Information can be recovered following a disaster or media failure; and

9.1.9 Protect paper records containing Protected Information from unauthorized access and other physical and environmental threats.

9.2 Changes to Shutterstock's organization, process, information processing facilities and systems that affect security must be reviewed prior to implementation and controlled. New information systems must be tested prior to acceptance and use.

9.3 Operating procedures, architectures, and data flows must be documented and made available to all Shutterstock personnel who require access to fulfill their role. These written procedures should document installation, configuration, maintenance/support, monitoring (availability & capacity, log reviews), backup and decommissioning based on risk of the resource to the organization.

10. **Access Control**

10.1 **Access to Protected Information**. Shutterstock will implement commercially reasonable practices and procedures designed, as appropriate, to limit and control access to Protected Information and to information systems used to Process or access such information. Such practices and procedures should be designed, as appropriate, to ensure that:

10.1.1 Personnel, Service Providers, and other third parties with regular access to Protected Information are informed about their responsibilities for safeguarding such information and the responsibility to limit access to both internal and external network services to avoid compromise of Protected Information stored on Shutterstock's network;

10.1.2 Personnel, Service Providers, and other third parties with access to systems used to Process Protected Information have unique user credentials so that each individual's access of Shutterstock information resources can be tracked across the network;

10.1.3 Personnel, Service Providers, and other third parties with regular access to Protected Information have a password, known only to that user, that will: (1) be sufficiently complex; (2) be changed periodically; (3) not be reused; (4) not be stored in login scripts or other computer programs; (5) be deactivated immediately if reported lost or compromised; and (6) never be written into any application software code;

10.1.4 Unattended equipment must be automatically locked after a reasonable period of inactivity and storage media containing Protected Information is not left unattended;

10.1.5 Access to Shutterstock systems must be restricted by (1) authenticating all users; (2) recording successful and failed system authentication attempts; (3) recording the use of special system privileges; (4) monitoring to detect actual and attempted attacks on or intrusions into systems containing Protected Information; (5) issuing alarms when system security policies, practices, and/or procedures are breached; (6) limiting user access to those network services necessary for the user's responsibilities; (7) cataloguing and monitoring connections to Shutterstock systems from external sources; and (8) restricting the connection time of users;

10.1.6 Access to system and application software is restricted for information systems used to Process or access Protected Information;

10.1.7 Remote access to systems used to Process or access Protected Information does not compromise the security of such information; and

10.1.8 Shutterstock periodically reviews the access control and privilege management practices and procedures that are designed to limit access to Protected Information.

11. **Protected Information Systems Acquisition, Development and Maintenance**

11.1 **Systems acquisition, development, and maintenance**. Shutterstock will use commercially reasonable practices and procedures designed to ensure that information systems used to Process or access Protected Information are acquired, developed, and maintained in a manner designed to safeguard that information.

11.1.1 **System requirements**. To the extent practicable, all security and privacy requirements will be identified and documented at the requirements phase of a project intended to facilitate storage of, access to, and/or Processing of Protected Information, including the concept of "Privacy by Design".

11.1.2 **Information processing**. To the extent practicable, appropriate security controls, including validation of input data, internal processing, and output data, will be designed into applications that will be used to access and/or Process Protected Information.

11.1.3 **Cryptographic controls**. Shutterstock will adopt practices and procedures to encrypt Protected Information stored on laptops, portable media, and/or transmitted over a wireless network or the public Internet.

11.1.4 **Technical vulnerability management**. Shutterstock will implement and regularly test and update practices and procedures designed to protect against risks related to published technical vulnerabilities associated with systems or applications used to Process or access Protected Information. Periodic audits should be conducted or reviewed by independent third parties.

12. **Information Security Incident Management**

12.1 **Incident response**. Shutterstock will implement and maintain commercially reasonable practices and procedures designed to enable Shutterstock to identify and respond in an appropriate manner to information security incidents involving Protected Information and/or information systems used to Process or access that information, including a procedure for the notification to the affected Data Subject(s) and/or Data Protection Authority in compliance with GDPR or other applicable law requiring notification to affected individuals or regulatory authorities.

12.2 Shutterstock will ensure that this Information Security Incident Management program can be scaled to handle any size or risk scenario and addresses the following elements to allow for effective and efficient information security incident handling:

12.2.1 Preparation and detection

12.2.2 Validation

12.2.3 Incident declaration

12.2.4 Containment

12.2.5 Recovery

12.2.6 Forensic investigation

12.2.7 communications/reporting

12.2.8 Post-mortem

12.3 **Event logs**. Shutterstock will maintain or cause to be maintained event logs recording user activities, exceptions, faults, and information security events, as well as logs with respect to system administrator and system operator activities. All such logs shall be protected and reviewed on a regular basis.

13. **Business Continuity Management**

13.1 **Information security aspects of business continuity management**. Shutterstock Personnel responsible for systems that Process Shutterstock Protected Information will take reasonable steps to minimize the impact of and facilitate recovery from loss of critical systems and Protected Information. Such steps will include practices and procedures designed to identify and reduce risks, prevent incidents, limit the consequences of damaging incidents, and ensure that Protected Information required for critical business processes is readily available.

14. **Reviews and Adjustments**

14.1 **Periodic re-evaluations**. The Chief Information Security Officer will re-evaluate and report to Senior Management regarding the Information Security Program on a periodic basis (at least once annually), taking into account changes in applicable technical standards and industry practice, and technology or other developments having a material impact on information security. Shutterstock's Legal Department will report to the relevant Senior Management, such as the Privacy Officer, Chief Information Security Officer, and Chief Operating Officer regarding changes in applicable legal or professional responsibility standards having a material impact on the security of Protected Information.

14.2 **Incident-related re-evaluations**. The Chief Information Security Officer will re-evaluate this Program and report any findings to the Privacy Officer and Chief Operating Officer whenever

its effectiveness is called into question by testing and monitoring, system failures, a material change in business operations, or technology changes or other developments having a material impact on any Protected Information and information systems used to Process or access that information.

14.3 **Modification**. Should the Chief Information Security Officer determine, based on review of any periodic or incident-related re-evaluation, that this Program should be modified, supplemented, or amended, the Chief Information Security Officer will recommend necessary modifications, supplements, or amendments.

14.4 **Independent review**. Shutterstock shall have its approach to managing information security and its implementation of the Program reviewed independently at planned intervals or when significant changes occur. The Chief Information Security Officer shall work with Senior Management to establish the requirements and timing for such reviews.

14.5 **Management reviews**. Managers shall regularly review the compliance of any information processing and procedures within their areas of responsibility with the Program and any related policies or other requirements and discuss any issues of concern with the Chief Information Security Officer, Privacy Officer, or Senior Management, as appropriate.

15. **Related Procedures and Subordinate Policies.** Shutterstock shall define, maintain, and train Shutterstock personnel, Service Providers, and other third parties on the Policies and Procedures that support the objectives of this Information Security Policy. These Policies and Procedures will be subject to periodic review (at least once annually), taking into account changes in applicable technical standards and industry practice, and technology or other developments having a material impact on information security.

16. **Compliance**

16.1 **Requirements**. The Chief Information Security Officer will work with Shutterstock's Compliance Officer to ensure that the Program meets Shutterstock's compliance requirements, including compliance with applicable intellectual property rights and obligations, record retention requirements, personal data protection and privacy laws and regulations, and contractual obligations.

16.2 Compliance with this Information Security Policy is mandatory for all Shutterstock personnel. Any non-compliance to this policy or related security policies shall be documented and reported to the Chief Information Security Officer for review.