DIGITAL PROMISE AND DIGITAL PROMISE GLOBAL

INFORMATION SECURITY POLICY

MARCH 27, 2018

Effective Date: April 27, 2018

CONTENTS

1. Purpose and Scope

1.1 Confidential Information. Digital Promise and Digital Promise Global (collectively, "DP" or "Digital Promise") regularly receives, stores, handles, and generates Confidential Information, including digital and electronic, about Digital Promise clients, consultants, contractors, employees, temporary staff, and Digital Promise's business (collectively, "Confidential Information"). Because of the central role such information can play in Digital Promise's objectives and mission, as well as the objectives and mission of Digital Promise's clients, consultants, contractors and other interested parties, Digital Promise seeks to safeguard all such information in its possession.

1.2 Organizational commitment to Information Security. DP is committed to safeguarding Confidential Information by adopting, implementing, and adhering to appropriate Controls, including policies, processes, procedures, organizational structures, and technology designed to safeguard Confidential Information.

1.3 Scope. This policy establishes procedures for protecting DP's Information Assets, including both Confidential Information and Information Systems.

2. Terms and Definitions

2.1 Capitalized Terms. Unless otherwise defined in the text of this Policy, capitalized terms shall have the meanings set forth in Appendix A.

3. Organization of Information Security

3.1 Responsibility for Information Security. Except as specified herein, implementation of this policy shall be the responsibility of the Information Officer ("IO"), subject to oversight by the Chief Operations Officer ("COO") and the Chief Executive Officer ("CEO") and subject to Approval. The COO shall report on the implementation of this policy as appropriate to the other members of Digital Promise.

3.1.1 Delegation. The IO will facilitate development and implementation of Information Security practices. The IO shall be empowered to develop, implement, and enforce, directly or indirectly, Information Security Controls and policies, including and in accordance with this Policy. The IO may delegate his or her duties under this Policy or in any Appendix hereto to Digital Promise Personnel (which Appendix A defines as including employees, temporary staff, consultants, and contractors working for Digital Promise) who report to the IO as appropriate.

3.1.2 Approval. The term "Approval" as used herein shall mean approval by the CEO of the specified Control, action, or expenditure by the COO of Digital Promise prior to such Control, action, or expenditure being taken.

3.2 Organization-wide support and coordination. The IO shall coordinate Information Security activities, involving representatives from different functions with relevant roles as appropriate. Other departments and functions shall support Digital Promise in this role.

Directors and Managers of these functions may have day-to-day responsibility for implementation of required Information Security Controls.

3.3 Communications regarding Information Security. The COO, in consultation with the IO, shall manage communications regarding security incidents and other security-related matters with law enforcement, regulatory officials, clients and others in accordance with the Data Security Incident Response Plan.

3.4 Special Interest Groups related to Information Security. The IO shall establish and maintain relationships with relevant special interest groups, vendors, and other business-related organizations in order to inform and be informed of new developments as they relate to Information Security.

4. Risk Assessment and Treatment

4.1 Assessing security risks. The IO shall conduct Risk Assessments to identify, quantify, and prioritize information security risks against criteria for risk acceptance that reflect Digital Promise's legal obligations, goals, and objectives.

4.2 Responding to identified security risks. For each risk identified, the IO shall propose, and, upon Approval, select and implement Controls as necessary and appropriate.

5. Information Asset Management

5.1 Inventory of Information Systems. The IO shall maintain an organization-wide inventory of important Information Assets.

5.2 Classification of Confidential Information. The IO shall develop and implement a classification scheme for Confidential Information.

5.3 Acceptable use of Information Assets. Upon Approval, the IO shall establish and implement rules for use of Digital Promise's Information Assets.

6. Human Resources Security

6.1 Initial Employment Training. The COO, with support of the IO, shall implement training to make Digital Promise Personnel aware of their obligations with respect to this Information Security Policy, including any Appendices hereto. Such training shall be provided to all current Digital Promise Personnel after the effective date of this Information Security Policy and, for new Digital Promise Personnel hired after the effective date, at the time of, and as a term and condition of, employment. All Digital Promise Personnel must be educated on the principles and procedures forth in this Policy, as applied to the specific context in which they handle Confidential Information and the nature of that Confidential Information. The training required by this Section 6.1 may be offered in conjunction with training required by the Digital Promise Privacy Policy.

6.2 During employment. The COO, with the support of the IO, shall implement "refresher" reminders or training annually, or in the event of material revisions to this Policy, to maintain awareness about Information Security procedures, including, but not limited to, the policies set forth in the Appendices hereto, and the protection of Confidential Information.

6.2.1 Education and training. Pursuant to such reminders or training, Digital Promise Personnel shall receive appropriate training, as applicable, and regular updates regarding organizational policies and procedures relevant for their job function.

6.3 Background checks. The COO shall cause background verification checks to be performed on all prospective employees of Digital Promise prior to employment, as applicable, and such background checks shall be carried out in accordance with applicable legal requirements.

6.4 Termination or change of status. The CEO and COO shall manage any separation of Digital Promise Personnel from Digital Promise so as to ensure the return or other disposition of all Confidential Information, information processing equipment, or other Digital Promise property. Relevant managers will be responsible for removing or modifying access rights upon an individual's separation or change of responsibilities.

7. Physical and Environmental Security

7.1 Secure areas. Policies governing secure areas are set forth in the Clean Desk Policy (Appendix E). The IO may create and maintain any additional measures as appropriate to protect against unauthorized access, alteration, or misuse of physical areas in which Information Assets are located, such as appropriate security perimeters, appropriate physical and electronic security barriers, and entry Controls. When appropriate, the IO should implement a system for logging access to facilities where Confidential Information is accessed, stored, and processed. The IO shall also propose and, upon Approval, implement measures to mitigate the risk to Information Assets from natural or man-made disasters in accordance with paragraph 14.1 of this Policy.

7.2 Equipment security. Policies governing equipment security are set forth in the Email Policy (Appendix B), the Password Guidelines (Appendix C), the Acceptable Use Policy (Appendix D), the Clean Desk Policy (Appendix E), the Software Installation Policy (Appendix F), the Remote Access Policy (Appendix G), and the Technology Equipment Disposal Policy (Appendix H). The IO may implement any additional reasonable measures as appropriate to protect organization-provided Information Assets, including that used offsite or remotely, from unauthorized access and other physical and environmental threats.

7.2.1 Equipment disposal or re-use. The IO shall securely erase all storage mediums, and dispose of computer equipment and other technology assets, in accordance with current reasonable industry practices.

7.3 Sending Confidential Information. The IO shall implement reasonable measures to ensure that Digital Promise Personnel do not send Confidential Information to third parties via unencrypted emails or third-party servers that are not encrypted or password protected.

7.4 De-Identification and Aggregation of data. The IO shall implement reasonable measures for de-identifying and aggregating data used for analytical, reporting, product development, research, or other appropriate purposes.

7.4.1 Removal of personal identifiers. De-identified data shall have all direct and indirect personal identifiers removed. This

includes, but is not limited to, name, ID numbers, date of birth, demographic information, location information, and school ID.

7.4.2 Prohibition on re-identifying data. Digital Promise Personnel and on-site Service Providers shall not attempt to re-identify de-identified data and not to transfer de-identified data to any party unless that party agrees not to attempt re-identification.

7.4.3 Aggregating Data. The IO shall implement reasonable measures to ensure that the aggregation of multiple individuals' Nonpublic Personal Information is sufficient to prevent identification of an individual from that data itself or in combination with publicly available data.

8. Service Delivery Management

8.1 Third-party service delivery management. The COO shall develop and implement processes designed to ensure that products and/or services shall be procured from Service Providers under terms and conditions designed to preserve the integrity and security of Information Assets. Such processes shall include:

8.1.1 Vetting. Digital Promise shall screen prospective Service Providers, who shall be required to conduct background verification checks on employees likely to have access to material Information Assets.

8.1.2 Security Assessment Questionnaire. Digital Promise shall provide a list of questions, if it determines they are necessary, as a means to review and assess the quality of data protection maintained and implemented by prospective Service Providers. The IO shall determine the appropriate questionnaire, if any, to use depending on the size of the Service Provider and the sensitivity of the information to be handled by the Service Provider.

8.1.3 Written contract. Digital Promise shall require Service Providers to agree in writing to safeguard Confidential Information before such Service Providers are permitted to access material Information Assets.

8.1.4 Responsibilities explained. Security responsibilities shall be explained to any Service Provider working on-site or having remote access to Information Assets, and any such Service Provider shall be required to acknowledge in writing its receipt and understanding of, and willingness to accept, such security responsibilities.

8.1.5 Monitoring program. Any access to Information Assets by Service Providers shall be authorized, documented, and appropriately limited. The IO shall review Service Provider access rights on a regular basis, commensurate with the sensitivity of the Confidential Information accessible by the relevant Service Provider.

8.1.6 Return or destroy. At the conclusion of its assigned tasks, Digital Promise shall require a Service Provider to return to Digital Promise or destroy any and all Confidential Information under its control, and to certify that it has purged its records and/or files of such Confidential Information.

8.1.6.a Outside Counsel. Outside counsel shall retain Digital Promise Confidential Information only for as long as specified by DP for the matters on which outside counsel is working or as otherwise necessary to satisfy the purposes for which it was provided to outside counsel, except to the extent that longer retention is required by applicable law, regulations, or professional ethical rules.

8.1.7 Improper Processing. Any Service Provider who Processes or attempts to Process Confidential Information without authorization or in a manner that violates security procedures shall be subject to contract termination and other appropriate legal action. In appropriate circumstances, the CEO or the COO may report violations of security procedures to government agencies, including law enforcement agencies.

9. Communications and Operations Management

9.1 System planning and acceptance. At such time that Digital Promise acquires systems to store Information Assets, the operational requirements of new systems shall be established, documented, and tested prior to their acceptance and use. The IO shall regularly update projections of future capacity requirements, and, upon Approval, adjust its procurement schedules accordingly, to reduce the risk of system overload.

9.2 Protection against malicious code. The IO shall implement and regularly update Controls to prevent the introduction of, detect the presence of, and remove malicious code on any systems acquired and used pursuant to Section 9.1, and Digital Promise Personnel with access to Information Assets shall be made aware of the dangers of malicious code pursuant to the training program set forth in paragraph 6.2.

9.3 Network security management. The IO shall implement Controls designed to safeguard information traversing system networks implemented pursuant to Section 9.1, and to protect connected services from unauthorized access.

9.3.1 Remote Access. In accordance with the Remote Access Policy (Appendix G), at such time as Digital Promise acquires and uses systems pursuant to Section 9.1, the IO and COO shall develop and make available an approved hardware and software list for remote access to DP's network and provide mandatory configuration procedures for each individual tool. This list should be limited to tools that can sustain a certain level of security, including, but not limited to, multi-factor authentication and end-to-end encryption.

9.4 Control of information media. Subject to Approval, the IO shall establish appropriate operating procedures to protect documents, computer media (e.g. tapes, disks), input/output data and system documentation from unauthorized disclosure, modification, removal, and destruction. Media shall be disposed of securely and safely when no longer required.

9.5 Exchange of information. Subject to Approval, the IO shall develop and make available to Digital Promise Personnel Controls to protect Confidential Information during transmission or exchange with Service Providers and other third parties, as well as Controls that Service Providers and other third parties must implement to protect Confidential Information at rest in their control. Such Controls shall be consistent with Digital Promise's legal obligations and organizational goals and objectives.

9.6 Monitoring. The IO shall monitor Information Systems, networks, and when appropriate, employee activity, and record Information Security events.

10. Access Control

10.1 External access to Information Assets. Subject to Approval, the IO shall establish and regularly update Controls to limit and control third-party access to Digital Promise's Information Assets.

11. Information Systems Acquisition

11.1 Information Systems. At such time that Digital Promise intends to acquire and implement an information system, Digital Promise shall modify this policy as appropriate to establish: (a) security requirements for such system, and (b) information processing, cryptographic, operating and system file, development and support process, technical vulnerability and management, and data retention and destruction Controls.

12. Data Retention and Destruction Control

12.1 Development of Retention and Destruction Policy. Subject to Approval, the IO shall develop and put into place appropriate Controls and procedures for the retention and destruction of Confidential Information. This policy shall address all documents of Digital Promise, including both electronic and paper files. Items that staff may not consider important, such as interoffice email, desktop calendars and printed memos are records that are considered important under this policy.

12.2 Retention. The length of time specific types of data are retained shall be guided by law where it is applicable and DP's Privacy Policy.

> **12.2.1** Destruction. While some data may simply be shredded or deleted from systems, for more sensitive data, stronger methods of destruction at a more granular level may need to be employed to assure that the data are truly irretrievable.

13. Information Security Incident Management

13.1 Reporting of Information Security Incidents and weaknesses. The reporting of Information Security Incidents shall be in accordance with the Data Security Incident Report Plan. With Approval, the IO may modify the plan as appropriate to implement any

additional reasonable procedures designed to ensure an effective and orderly response to Information Security Incidents. The IO shall be promptly informed of any Information Security incidents.

13.2 Responsibility for Incident and Weakness Reporting. Digital Promise Personnel, Service Providers, and any third party with access to Information Assets shall be required to report any Information Security Events or weaknesses to a designated point of contact or the IO.

14. Business Continuity Management

14.1 Information Security aspects of business continuity management. The COO shall propose, and upon Approval, implement and regularly test and update a business continuity management process designed to minimize the impact on Digital Promise and recover from loss of Information Assets, whether resulting from natural disasters, accidents, equipment failures, deliberate actions, or other causes.

14.2 Scope. This process shall include Controls designed to identify and reduce risks, prevent incidents, limit the consequences of damaging incidents, and ensure that information required for business processes is readily available.

14.3 Integration with general business continuity Controls. This process shall identify the critical business processes and integrate the Information Security management requirements of business continuity with other continuity requirements relating to such aspects as operations, staffing, materials, transport and facilities.

14.4 Backup. Digital Promise shall secure back-up facilities designed to mitigate the risk of loss of essential Information Assets following a disaster or media failure.

15. Compliance

15.1 Legal compliance. Digital Promise shall review legal and contractual obligations with respect to Information Security and shall implement Controls and procedures as appropriate.

15.2 Technical and policy compliance audit. The IO shall regularly review, assess, and audit Information Systems for compliance with applicable security policies, implementation standards, and documented security Controls, and shall report the results of such audit to the COO and CEO. Digital Promise shall periodically update and enhance its security policies, implementation standards, and documented security Controls.

16. Compliance with Third-Party Mandated Controls

16.1 Compliance with Third-Party Mandated Controls. Third parties may, from time to time, seek reasonable additional Controls with respect to Confidential Information in Digital Promise's possession. Such requests shall be reviewed by the IO who shall make a recommendation as to whether, and how, such additional Controls should be implemented. Upon agreement between Digital Promise and the third party and Approval of such additional Controls, Digital Promise shall establish procedures and protocols for the implementation of such Controls consistent with the other requirements of this Policy.

17. Compliance with Child Safeguarding Policy and Child Protection Laws

17.1 Compliance with Child Safeguarding Policy and Procedures. The IO and COO shall review the Child Safeguarding Policy and Procedures ("DPCSPP") (http://digitalpromise.org/wp-content/uploads/2016/03/Safeguarding-Children-Policy.pdf) and determine if any Controls are required to be developed and implemented to ensure compliance with the DPCSPP.

17.2 Compliance with FERPA and PPRA. The IO and COO shall determine if any Controls are required to be developed and implemented to ensure compliance with the Family Educational Rights and Privacy Act ("FERPA") and the federal Protection of Pupil Rights Amendment ("PPRA"), to the extent applicable to the work and activities of Digital Promise Representatives. This includes, but is not limited to the development and implementation of data de-identification techniques that effectively eliminates all direct student identifiers, as well as effectively mitigates the risk that indirect student identifiers could be used to reliably re-identify individual students. These techniques may include, but are not limited to masking, blurring, perturbation, record coding, redaction, and suppression.

17.3 Compliance with Laws, Regulations and Rules for Behavioral Research. The IO and COO shall determine if any Controls are required to be developed and implemented to ensure compliance with security laws, regulations and rules governing behavioral research involving human subjects, including, but not limited to, the Federal Policy for the Protection of Human Subjects (commonly referred to as the "Common Rule").

18. Insurance

18.1 Maintenance and Review of Insurance. To the extent that such insurance is reasonably commercially available, Digital Promise shall retain insurance with respect to its Information Assets and any Information Systems it may acquire and implement, including business loss and liability insurance related to Information Security Events and Information Security Incidents. The COO and IO shall, from time to time, as appropriate, review Digital Promise's insurance policies and make recommendations to the CEO, as appropriate, with respect to any proposed adjustments in such insurance.

19. Adjustment of this Policy

19.1 Periodic re-evaluations. The IO, COO, and CEO shall re-evaluate this Policy, including the Appendices, on a periodic basis, taking into account changes in legal or contractual obligations, changes in applicable technical standards and industry practice, and technology or other developments having a material impact on Information Security.

19.2 Modification. Following such periodic or other re-evaluation, Digital Promise shall modify, supplement, or amend this Policy as appropriate.

20. Digital Promise Personnel Compliance

20.1 Compliance Measurement. The IO and other staff may verify compliance to this policy and the Appendices through various methods, including but not limited to, periodic

walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback from employees or other third parties.

20.2 Exceptions. Any exception to the policy must be approved by the IO in advance.

20.3. Non-Compliance. Digital Promise Personnel who violate this Policy or the attached Appendices, or attempts to process or use Confidential Information or Information Systems without authorization, in excess of authorization, or in a manner that violates security procedures, may be subject to appropriate disciplinary action, which may include termination of employment, termination of a work assignment or contract, as applicable, and/or legal action. When deemed appropriate, the CEO may report violations of security procedures to appropriate outside organizations, including law enforcement authorities.

Appendix A: Terms and Definitions

Access Control	Means of insuring that only authorized users have access to information and information systems, on a need-to-know basis
Confidential Information	Nonpublic or Confidential information of third parties with which DP conducts business, including nonpublic or confidential information of other parties which such third parties provide to DP and, as defined in Digital Promise's Privacy Policy for Personal Information, Nonpublic Personal Information ("NPI") (collectively, "Third-Party Information"); Information that identifies or can be used to identify individuals who are or were employees of, or applicants for employment by, DP, or their dependents or beneficiaries ("Human Resources Information"); Information relating to DP's planned or existing information technology systems and systems architecture, including computer hardware, computer software, source code, object code, documentation, methods of processing and operational methods ("Technical Information"); Non-public business and organizational information relating to DP, including information about its finances, plans, strategies, organizational structure, personnel, and business initiatives ("Business Information"). Business information includes: Non-public information that describes DP's services, and how such services are administered and managed; and Any information that a reasonable person familiar with DP's organization would consider confidential or proprietary, the maintenance of which would be important to DP, its clients, contractors and consultants, and its employees; and any other information designated in writing as confidential by DP.
Control	Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature; control is also used as a synonym for safeguard or countermeasure.
Digital Promise Personnel	Employees, temporary staff, consultants, contractors working for Digital Promise.
Information Asset	Any data, Digital Promise-owned device, or other Digital Promise-owned component of Digital Promise's technology environment that supports information-related activities

Information Security	Protection of Confidential Information from a wide range of threats in order to ensure organizational continuity and minimize organizational risk
Information Security Event	An identified occurrence of a system, service or network state indicating a possible breach of Information Security policy or failure of safeguards, or a previously unknown situation that may be security relevant
Information Security Incident	Indicated by a single or a series of unwanted or unexpected Information Security events that have a significant probability of compromising organization operations and threatening Information Security
Information Systems	All hardware, software, and other technology tools on which Information Assets are processed or reside
Process Information	To receive, store, handle, or generate information
Risk Analysis	Systematic use of information to identify sources and to estimate risk
Risk Assessment	Overall process of risk analysis and risk evaluation
Risk Evaluation	Process of comparing the estimated risk against given risk criteria to determine the significance of the risk
Risk Treatment	Process of selection and implementation of measures to modify risk
Service Provider	Any individual, entity, or agent of an entity, that receives, maintains, Processes, or otherwise is permitted to access Confidential Information through its provision of services to Digital Promise.