

DATA PRIVACY AGREEMENT

Lancaster Central School District

This Data Privacy Agreement ("DPA") is by and between the **Lancaster Central School District** ("EA"), an Educational Agency, and Digital Inspiration

("Contractor"), collectively, the "Parties".

ARTICLE I: DEFINITIONS

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

- 1. Breach:** The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information in a manner not permitted by State and federal laws, rules and regulations, or in a manner which compromises its security or privacy, or by or to a person not authorized to acquire, access, use, or receive it, or a Breach of Contractor's security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personally Identifiable Information.
- 2. Commercial or Marketing Purpose:** means the sale, use or disclosure of Personally Identifiable Information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of Personally Identifiable Information for advertising purposes; or the sale, use or disclosure of Personally Identifiable Information to develop, improve or market products or services to students.
- 3. Disclose:** To permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written or electronic, whether intended or unintended.
- 4. Education Record:** An education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
- 5. Educational Agency (EA):** As defined in Education Law 2-d, a school district, board of cooperative educational services, school, charter school, or the New York State Education Department.
- 6. Eligible Student:** A student who is eighteen years of age or older.
- 7. Encrypt or Encryption:** As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304, means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.
- 8. NIST Cybersecurity Framework:** The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
- 9. Parent:** A parent, legal guardian or person in parental relation to the Student.

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

ARTICLE II: PRIVACY AND SECURITY OF PII

1. Compliance with Law

In order for Contractor to provide certain services ("Services") to the EA pursuant to date services begin 05/16/22 [date agreement is signed will populate upon signature]; Contractor may receive PII regulated by applicable New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); New York Education Law Section 2-d; and the Commissioner of Education’s Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements of New York law. Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federal and local laws, rules and regulations.

2. Authorized Use

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

3. Data Security and Privacy Plan

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

4. EA's Data Security and Privacy Policy

State law and regulation requires the EA to adopt a data security and privacy policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST Cyber Security Framework.

5. Contractor's Employees and Subcontractors

- (a) Contractor shall only disclose PII to Contractor's employees and subcontractors who need to know the PII in order to provide the Services and the disclosure of PII shall be limited to the extent necessary to provide such Services. Contractor shall ensure that all such employees and subcontractors comply with the terms of this DPA.
- (b) Contractor must ensure that each subcontractor performing functions pursuant to this DPA where the subcontractor will receive or have access to PII are consistent with those found in this DPA.
- (c) Contractor shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. In the event there is an incident in which the subcontractor compromises PII, Contractor shall follow the Data Breach reporting requirements set forth herein.
- (d) Contractor shall take full responsibility for the acts and omissions of its employees.
- (e) Contractor must not disclose PII to any unauthorized party unless such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the EA of the court order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the PII is disclosed, unless such disclosure to the EA is expressly prohibited by the statute, court order or subpoena.

6. Training

To the extent required by law, the contractor shall ensure that all its employees and subcontractors who have access to PII have received or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access.

7. Termination

The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its subcontractors retain PII or retain access to PII pursuant to the service agreement. Contractor will automatically delete all PII from its servers after a period of two (2) years following termination of the subscription, and from all backup servers after two (2) additional weeks. The EA may use the administrator portal to delete all PII at any time or may request assistance from Contractor to delete PII at any time. The confidentiality and data security

obligations of the Contractor under this DPA shall survive any termination of this DPA but shall terminate upon deletion of PII from both active servers and backups.

8. Data Return and Destruction of Data

- (a) Protecting PII from unauthorized access and disclosure is of the utmost importance to the EA, Contractor agrees that it is prohibited from retaining PII or continued access to PII or any copy, summary or extract of PII, on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever beyond the period prescribed by this agreement, or as expressly requested by the EA for purposes of facilitating the transfer of PII to the EA or expressly required by law. The EA may use the administrator portal to delete PII at any time or may request assistance from Contractor to do so. If not deleted by the EA, Contractor will automatically delete all PII from its servers after a period of no more than two (2) years following termination of the subscription, and from all backup servers after two (2) additional weeks.
- (b) With regard to all PII (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any and all PII maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Subcontractors, Contractor shall ensure that PII is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed. Hard copy media must be shredded or destroyed such that PII cannot be read or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. Only the destruction of paper PII, and not redaction, will satisfy the requirements for data destruction. Redaction is specifically excluded as a means of data destruction.
- (c) Upon request, Contractor shall provide the EA with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.
- (d) To the extent that Contractor and/or its subcontractors continue to be in possession of any de-identified data (i.e., data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data.

9. Commercial or Marketing Use Prohibition

Contractor agrees that it will not sell PII or use or disclose PII for a Commercial or Marketing Purpose, except that teachers may receive email communications regarding product updates or professional development opportunities from which they may opt out at any time.

10. Encryption

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

11. Breach

- (a) Contractor shall promptly notify the EA of any Breach of PII without unreasonable delay no later than seven (7) calendar days after discovery of the Breach. Notifications required pursuant to this section must be in writing, given by personal delivery, e-mail transmission (if contact information is provided for the specific mode of delivery), or by registered or certified mail, and must to the extent available, include a description of the Breach which

includes the date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Contractor's investigation; and the contact information for representatives who can assist the EA. Notifications required by this section must be sent to the EA's District Superintendent or other head administrator with a copy to the Data Protection Office. Violations of the requirement to notify the EA shall be subject to a civil penalty pursuant to Education Law Section 2-d. The Breach of certain PII protected by Education Law Section 2-d may subject the Contractor to additional penalties.

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

Michele Ziegler,
Data Protection Officer/Director of Instructional Technology and Accountability
Lancaster Central School District
177 Central Avenue
Lancaster, NY 14086
mziegler@lancasterschools.org

12. Cooperation with Investigations

Contractor agrees that it will cooperate with the EA and law enforcement, where necessary, in any investigations into a Breach of data governed by this DPA.

13. Notification to Individuals

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

ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS

1. Parent and Eligible Student Access

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

2. Bill of Rights for Data Privacy and Security

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

ARTICLE IV: MISCELLANEOUS

1. Priority of Agreements and Precedence

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

2. Execution

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


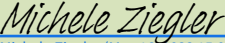
Contractor Name: Digital Inspiration	
Signature:	 <small>Amit Agarwal (May 16, 2022 19:42 GMT+5.5)</small>
Printed Name:	Amit Agarwal
Title:	Founder
Email:	amit@labnol.org
Date:	05/16/22
Lancaster Central School District Data Protection Officer – Michele Ziegler	
Date: May 16, 2022	Signature:  <small>Michele Ziegler (May 16, 2022 15:08 EDT)</small>

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

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

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

The Lancaster Central School District is committed to protecting the privacy and security of student protected data and teacher and principal data. In accordance with New York Education Law Section 2-d and its implementing regulations, the District informs the school community of the following:

1. A student's personally identifiable information cannot be sold or released for any commercial purpose.
2. Parents have the right to inspect and review the complete contents of their child's education record.
3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices including, but not limited to encryption, firewalls, and password protection, must be in place when data is stored or transferred.
4. A complete list of all student protected data elements collected by New York State (<http://www.nysed.gov/data-privacy-security/student-data-inventory>) is available for public review or by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, New York 12234.
5. Parents have the right to submit complaints about possible breaches of student protected data or teacher or principal Annual Professional Performance Review data. Any such complaint must be submitted, in writing, to: Michele Ziegler, Director of Instructional Technology, 177 Central Avenue, Lancaster, New York 14086. Additionally, parents have the right to have complaints about possible breaches of student protected data addressed. Complaints should be directed to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234; the email address is "cpo@mail.nysed.gov". The State Education Department's complaint process is under development and will be established through regulations from the department's chief privacy officer, who has yet to be appointed.

Supplemental Information Regarding Third-Party Contractors

In the course of complying with its obligations under the law and providing educational services to District residents, the Lancaster Central School District has entered into agreements with certain third-party contractors. Pursuant to these agreements, third-party contractors may have access to "student data" and/or "teacher or principal data," as those terms are defined by law and regulation.

For each contract or other written agreement that the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data from the District, the following supplemental information will be included with this Bill of Rights:

1. The exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor;
2. How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable laws and regulations (e.g., Family Educational Rights and Privacy Act; Education Law Section 2-d);
3. The duration of the contract, including the contract’s expiration date, and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when, and in what format it will be returned to the District, and/or whether, when, and how the data will be destroyed);
4. If and how a parent, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data that is collected;
5. Where the student data or teacher or principal data will be stored, described in a manner as to protect data security, and the security protections taken to protect the data privacy and mitigate security risks; and
6. Address how the data will be protected using encryption while in motion and at rest.


Contractor Name: Digital Inspiration	
Signature:	 <small>Amit Agarwal (May 16, 2022 19:42 GMT+5.5)</small>
Printed Name:	Amit Agarwal
Title:	Founder
Email:	amit@labnol.org
Date:	05/16/22

EXHIBIT B – Bill of Rights for Data Privacy and Security

Supplemental Information for Contracts That Utilize Personally Identifiable Information

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

Description of the purpose(s) for which Contractor will receive/access PII	The exclusive purpose for which Vendor is receiving Protected Data from the District is to provide the district with functionality of the product or services listed above. Vendor will not use the Protected Data for any other purposes not explicitly authorized above or within the Master Agreement.
Type of PII that Contractor will receive/access	Check applicable options: <input type="radio"/> Student PII <input type="radio"/> BOTH Student PII and APPR Data <input checked="" type="radio"/> APPR Data
Contract Term	Start Date: <u>05/16/22</u> End Date: Agreement remains in effect as long as the account is current and in good standing or upon expiration of the master agreement without renewal, or upon termination of the master agreement prior to its expiration.
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) <input type="radio"/> Contractor will not utilize subcontractors. <input checked="" type="radio"/> Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: <input type="radio"/> Securely transfer PII to EA, or a successor contractor at the EA’s option and written discretion, in a format agreed to by the parties. <input checked="" type="radio"/> Securely delete and destroy PII.
Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify the Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA’s written request.
Secure Storage and Data Security	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply) <input type="radio"/> Using a cloud or infrastructure owned and hosted by a third party. <input checked="" type="radio"/> Using Contractor owned and hosted solution <input type="radio"/> Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:
Encryption	Data will be encrypted while in motion and at rest.

EXHIBIT B – Bill of Rights for Data Privacy and Security


Contractor Name: Digital Inspiration	
Signature:	 <small>Amit Agarwal (May 16, 2022 19:42 GMT+5.5)</small>
Printed Name:	Amit Agarwal
Title:	Founder
Email:	amit@labnol.org
Date:	05/16/22

EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. **For every contract, the Contractor must review the following list and provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York State.**

CONTRACTORS ATTACHED PLAN SHALL INCLUDE THE FOLLOWING:

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.
7	Describe your secure destruction practices and how certification will be provided to the EA.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 https://www.nist.gov/cyberframework/new-framework



Information Classification and Handling Policy

Document Owner

Amit Agarwal
Digital Inspiration

Owner Contact

amit@labnol.org

91-9760008595

Effective Date

March 01, 2021

Version Number:

1.0

CONTENTS

Overview	2
Governance Terms	2
Information Classification and Handling	5
Appendix A Definitions	13
Appendix B Revision History	15
Appendix C Framework Reference	16

OVERVIEW

Digital Inspiration is providing requirements and guidance for safeguarding Digital Inspiration assets in the form of policies, standards, and guidelines. This governance supports Digital Inspiration security goals, which in turn support the growth and strategy of the entire organization.

This document supports the following Digital Inspiration goals:

- Implement governance that supports the business goals of Digital Inspiration.
- Create documented security statements that reflect Digital Inspiration’s requirements and guidance for information security.
- Protect sensitive or confidential information.
- Establish accountability for protecting Digital Inspiration’s information assets.
- Avoid security incidents.

Governance Terms

The following terms are used throughout this document. Defining these terms establishes a common approach for their use and facilitates compliance.

Term	Definition
Governance	Corporate governance is a system of rules by which a company is governed. Governance includes policies, standards, and guidelines.
Policy	<p>An information security policy is a high-level, mandatory statement that provides Digital Inspiration’ requirements with regard to security. A policy does not address the details of how something should be done. Rather, policies provide guidance for the creation of supporting standards, procedures, and guidelines.</p> <p>Example: “IT SUPPORT shall configure workstations to authenticate users.”</p>
Standard	<p>A standard is a lower-level mandatory statement than a policy that also addresses what must be done, but not necessarily how it must be done. Standards are largely technology-specific, and often include the pseudo-code for configuration that will be translated into the actual code in the procedures. In many cases, standards are tiered.</p> <p>A baseline standard provides the minimum requirements for a particular component or area. A specific standard may detail the requirements for a certain type of device or a device in a certain environment.</p>

Example: "IT SUPPORT shall configure workstations to require a 10 character, alphanumeric password that is different from the user's Google account."

Guideline Guidelines are recommendations from Digital Inspiration's executive management that help support standards. Guidelines are not mandatory requirements.

Example: "Use a phrase to create a long, complex password, capitalizing the first letter of each word."

Procedure Procedures are step-by-step instructions for how to implement what is required by the policies and standards. Procedures can be technical, as in the case of a configuration checklist for securing a particular piece of infrastructure, or process based, as in the case of a change management procedure.

Example: "To log in to your workstation:

1. In the User account field, enter the user account you received from Corporate IT.
2. In the Password field, enter the temporary password you received from DESKTOP SUPPORT.
3. Hit enter.
4. You will receive a prompt to change your password. Enter your new password at the prompt."

Process A process is a series of steps demonstrating how a goal is achieved.

These are generally illustrated by a diagram that shows responsibilities for each step, decision points, and alternatives, along with a description of what is happening at each step.

Example: "The request for a new user starts when HR enters a new employee or contractor in the HR system. The HR system generates a ticket to request the account.

- If the account is for an employee...
- If the account is for a contractor...

Plan A plan is an approach to get from one state to another, in alignment with the strategy. Whereas the strategy defines the goals, the plan describes how to get there. An annual plan helps Digital Inspiration achieve its goals within that time frame.

The core security plans that all organizations must have include:

- Disaster recovery plan
- Business continuity plan
- Security incident response plan

Organizations that use personal information must also have a privacy incident response plan.

Information Classification and Handling

Purpose

To protect information based on its sensitivity and importance to the organization

Scope

All Digital Inspiration physical and electronic information

Accountabilities

- All personnel - Responsible
- Legal - Responsible, Accountable, Consulted
- Executives - Responsible, Accountable, Consulted
- Security - Responsible, Consulted
- Technical Engagement Managers - Responsible

Requirements

Information Owners shall classify information assets and the assets that store, process, transport, or otherwise handle or protect the asset based on legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification. All Digital Inspiration personnel with questions about the information classification of a specific data element or information asset shall contact INFOSEC.

The following table defines each of the classifications and provides illustrative examples of each.

Classification	Definition	Illustrative Examples
Confidential	<ul style="list-style-type: none">Information intended for use only by specific individuals on a need-to-know basisInformation protected by law, contractual obligation, or policyInformation with the potential for severe negative repercussions to Digital Inspiration's reputation, resources, services, or individuals if disclosed	<ul style="list-style-type: none">Sensitive personal information about customers, whether or not it is tied to identifying information including financial informationData "en masse," such as ALL customer names or ALL phone numbersPasswords, PINs, access codes, security codesEmployee recordsCorporate financial informationNetwork diagrams and other system information
Internal	<ul style="list-style-type: none">Information intended for Digital Inspiration use onlyNon-public information that does not reach the sensitivity of Confidential	<ul style="list-style-type: none">Usage information about customer actions on the Digital Inspiration site, such as viewing a page, trying to sign up, or accepting a credit card offer, in conjunction with identifiable information

	<ul style="list-style-type: none"> Information with the potential for moderate negative repercussions to Digital Inspiration's reputation, resources, services, or individuals if disclosed 	<ul style="list-style-type: none"> "In wallet" information, such as a user's address, phone number, email address, or name¹ Publicly posted content, such as customer reviews on an item Confluence Contracts
Public	<ul style="list-style-type: none"> Information intended to be publicly available Information that poses little or no risk to Digital Inspiration's reputation, resources, services, or individuals if disclosed 	<ul style="list-style-type: none"> Customer information that is publicly available or in an aggregate form that cannot be identified to a particular individual Job postings Blog Posts Corporate contact information Corporate address Public facing web pages Press releases

Confidential Information

The table below lists all data elements that Digital Inspiration classifies as "Confidential," and under what circumstances the data element is Confidential.

- The "Isolated" column explains the classification of the data element if it is not listed with any other data elements.
- The "Aggregated" column lists data elements which, when combined with the listed data element, make the data element Confidential.

Data Element	Isolated	Aggregated (Confidential)
Address	Public	<ul style="list-style-type: none"> Name and email Name and phone number
Name	Public	<ul style="list-style-type: none"> Address and email

¹Only applies to individual or small numbers of users. Large sets of user data, such as ALL phone numbers in the database, must be treated as "Confidential."

Information Handling

Digital Inspiration shall handle information assets in accordance with their information classification, including how information is labeled, how removable media is managed, and how electronic storage media is destroyed.

INFOSEC shall define requirements for the levels of protection for information assets based on the needs for confidentiality, integrity, and availability of those assets. INFOSEC and LEGAL shall define legal and contractual requirements.

All Digital Inspiration personnel with questions about how to handle a specific information asset shall contact INFOSEC.

Information Handling Chart

The chart below summarizes the requirements for handling information based on classification. Information commingled with multiple classifications must always be handled with the highest applicable classification (e.g. public information that is stored or transmitted along with Confidential information may be encrypted in order to simplify the use of encryption solutions).

Confidential	
Distribution	<ul style="list-style-type: none">▪ Not shared with third parties▪ Customer information never included in reports, regardless of accompanying data
Labeling	<ul style="list-style-type: none">▪ Documents, spreadsheets, presentations² and text files labeled “Confidential³”▪ All paper documents labeled “Confidential”
Paper documents	<ul style="list-style-type: none">▪ Only printed when there is a legitimate business need and no reasonable alternative, with management approval▪ Stored in a locked cabinet▪ Placed in destruction bin for shredding immediately after use
Electronic files	<ul style="list-style-type: none">▪ Collected or stored when there is a legitimate business need and no reasonable alternative, with management approval▪ Stored and transmitted encrypted⁴▪ Wiped from electronic media immediately after use⁵
Internal	
Distribution	<ul style="list-style-type: none">▪ Redistributed to anyone within Digital Inspiration
Labeling	<ul style="list-style-type: none">▪ Not labeled
Paper documents	<ul style="list-style-type: none">▪ Only printed when there is a legitimate business need and no reasonable alternative▪ Stored on Digital Inspiration premises or in locked cabinet▪ Placed in destruction bin for shredding immediately after use
Electronic files	<ul style="list-style-type: none">▪ Stored and transmitted in clear text on Digital Inspiration corporate systems▪ Deleted or wiped from electronic media immediately after use
Public	
Distribution	<ul style="list-style-type: none">▪ Shared with anyone internal or external to Digital Inspiration
Labeling	<ul style="list-style-type: none">▪ Not labeled
Paper documents	<ul style="list-style-type: none">▪ Recycled conventionally when no longer needed
Electronic files	<ul style="list-style-type: none">▪ Stored and transmitted in clear text▪ Deleted or wiped from electronic media immediately after use

² I.e. Word, Excel, PowerPoint, Visio, and similar files

³ See Labeling standard for labeling requirements.

⁴ See Encryption Management standard for encryption requirements.

⁵ See Media Sanitation standard for wipe requirements.

Verbal Communication

Personnel shall use caution when discussing Confidential or Internal information in public locations, and shall not leave Confidential or Internal Information in voice mails.

Off-Site Assets

Personnel shall not leave Digital Inspiration Internal or Confidential information assets unattended in public locations.

Removable Media

The transfer of Internal and Confidential information to removable media must be authorized by INFOSEC. Management shall monitor the use of any authorized removable media to verify that it is handled according to the Asset Handling standard.

IT SUPPORT shall provide removable media with an approved request. All removable media must be company-supplied; no personal removable media may be used on the Digital Inspiration network.

All removable media that contains Internal or Confidential information must be stored in a locked cabinet or similarly restricted location when not in use.

The table below summarizes the required protection methods for each media type and classification.

Media Type	Protection Method		
	Confidential	Internal	Public
Backup tapes	Encrypted ⁶	Encrypted	Encrypted
CDs or DVDs	Not stored	Not stored	Stored in clear text
USB removable media (thumb drives, pen drives, flash drives, USB hard drives, removable backup drives)	Not stored	Not stored	Stored in clear text

Physical media must be sent using an approved courier⁷.

Facsimile Machines

Internal and Confidential information may not be sent via facsimile (fax) machines.

Enforcement

COMPLIANCE shall monitor compliance as an integrated part of routine assessments.

COMPLIANCE shall monitor compliance with this policy as an integrated part of routine assessments.

⁶ See Encryption Management standard for encryption requirements.

⁷ See the Third Party Relationship Management policy and standards for vendor approval requirements.

Standards

Labeling

Format	Requirement
Electronic files	<p>Documents, spreadsheets, and presentations⁸ containing Confidential information must be labeled “Confidential” in the header or footer with a minimum font size of eight (8). Text files containing Confidential information must be labeled “Confidential” at the top of the first page.</p> <p>Documents, spreadsheets, presentations, and text files must have the acronym “HC” in the file name.</p> <p>Databases, applications, and backup media do not require a label.</p>
Paper documents	<p>Paper documents that do not have the “Confidential” label printed in the header or footer must be stamped “Confidential” immediately after printing, using one of the stamp pads located by each printer.</p>

Media Sanitation

Personnel shall turn in all end-of-life media to INFRASTRUCTURE. INFRASTRUCTURE shall destroy all end-of-life media as follows:

Media Type	Sanitation Method		
	Confidential	Internal	Public
Apple iPhone and iPad	Shred, incinerate, or pulverize	Select the full sanitize option ⁹	Select the full sanitize option ¹⁰
Backup tapes	Shred, incinerate, or pulverize	(See Confidential)	(See Confidential)
Blackberry	Shred, incinerate, or pulverize	Perform a wipe ¹¹	Perform a wipe ¹²
CDs or DVDs	Place in a shred bin	Place in a shred bin	Recycle

⁸ I.e. Word, Excel, PowerPoint, Visio, and similar files

⁹ The full sanitize option is typically located in “Settings>General>Reset>Erase All Content and Settings.”

¹⁰ The full sanitize option is typically located in “Settings>General>Reset>Erase All Content and Settings.”

¹¹ In Blackberry OS 7.x and 6.x, select “Select Options>Security>Security Wipe, select all subcategories of data types for sanitation. Then type “blackberry” in the text field, and click on “Wipe” (or “Wipe Data in OS 6.x) For OS 10.x, select “Settings>Security and Privacy>Security Wipe. Type “blackberry” in the text field, then click on “Delete Data.”

¹² In Blackberry OS 7.x and 6.x, select “Select Options>Security>Security Wipe, select all subcategories of data types for sanitation. Then type “blackberry” in the text field, and click on “Wipe” (or “Wipe Data in OS 6.x) For OS 10.x, select “Settings>Security and Privacy>Security Wipe. Type “blackberry” in the text field, then click on “Delete Data.”

Google Android, Windows, and other mobile devices	Shred, incinerate, or pulverize	Varies by device manufacturer; contact INFOSEC	Varies by device manufacturer; contact INFOSEC
Hard Drives (ATA and SCSI)	Shred, incinerate, or pulverize	Shred, incinerate, or pulverize	Shred, incinerate, or pulverize
Network Devices	Shred, incinerate, or pulverize	Shred, incinerate, or pulverize	Shred, incinerate, or pulverize
USB removable media (thumb drives, pen drives, flash drives, USB hard drives, removable backup drives)	Shred, incinerate, or pulverize	Overwrite media using approved Sanitation Software ¹³	Overwrite media using approved Sanitation Software ¹⁴

INFRASTRUCTURE shall obtain destruction certificates for all destroyed media containing Confidential information. COMPLIANCE shall retain these destruction certificates.

¹³ See Appendix C – Tools and Services for approved Sanitation Software.

¹⁴ See Appendix C – Tools and Services for approved Sanitation Software.

APPENDIX A DEFINITIONS

The table below explains the terms used in this document.

Term	Definition
Data Element	A data element is a unit, field, or range of values that conveys meaningful information. Examples of data elements are name, address, and account number.
Enterprise	The Digital Inspiration enterprise refers to the entire organization.
Hardware	Hardware is physical equipment that is used to store, process, or transmit information.
Information Asset	An information asset is an electronic system that is used to store, process, or transmit information.
Information Asset Owner	An Information Asset Owner is an employee who has accountability and decision-making authority for an information asset.
Information Security (InfoSec)	Information security is the practice of protecting the confidentiality, integrity, and availability of information.
Management	Management refers to the heads of departments at the Director level and above.
Personnel	Personnel are individuals working at Digital Inspiration, including all employees, vendors, and contractors.
Personally Identifiable Information (PII)	PII is information that can be used either on its own or with other information to identify, contact, or locate a single individual, or to identify an individual in context.
Procedure	Procedures are step-by-step instructions for how to implement what is required by the policies and standards. Procedures can be technical, as in the case of a configuration checklist for securing a particular piece of infrastructure, or process-based, as in the case of a change management procedure.
Process	<p>A process is a series of steps demonstrating how a goal is achieved.</p> <p>These are generally illustrated by a diagram that shows responsibilities for each step, decision points, and alternatives, along with a description of what is happening at each step.</p>
Risk	Risks are potential events with a negative impact on the integrity, availability or confidentiality of data and or to the reputation of Digital Inspiration. Risks could also subject Digital Inspiration to legal sanctions.

Security Weakness

A security weakness is a flaw that could potentially lead to a compromise of the confidentiality, integrity, or availability of a Digital Inspiration information asset.

System

System is a category that includes all hardware, software, firmware, middleware, and electronic devices at Digital Inspiration.

APPENDIX B REVISION HISTORY

This table lists each revision of Digital Inspiration's security policies and standards, along with details about what was changed, who made the changes, and the date that those changes were effective (i.e. approved by the [Security Council](#)). For information on maintaining this document, see the [Governance Design and Maintenance](#) policy.

Revision	Changes and Updates Since Previous Versions	Author	Effective Date
1.0	First version	Amit Agarwal Founder, Digital Inspiration	March 01, 2021

APPENDIX C FRAMEWORK REFERENCE

Digital Inspiration's security policies and standards are based on the International Standard Organization's (ISO) standards 27002:2013. References to ISO standards are marked throughout the document and are summarized below, followed by page numbers.

ISO Reference	Page Number
ISO 27002 11.2.6	9
ISO 27002 13.2.1	9
ISO 27002 8.2.1	5
ISO 27002 8.2.2	7, 8, 11
ISO 27002 8.2.2, 8.3.1, 8.3.2, 8.3.3, 11.2.7	7
ISO 27002 8.2.3, 11.2.5	7
ISO 27002 8.3.1	9
ISO 27002 8.3.2, 11.2.7, NIST 800-88	11
ISO 27002 8.3.3	9