

# 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).

<b>Name of Contractor</b>	Media Flex Inc. _____
<b>PII Declaration</b>	<p><b>Does your organization/software collect student personally identifiable information (PII) or staff PII?</b></p> <p>Examples of student PII:</p> <ul style="list-style-type: none"> <li>a. The student's name;</li> <li>b. The name of the student's parent or other family members;</li> <li>c. The address of the student or student's family;</li> <li>d. A personal identifier, such as the student's social security number, student number, or biometric record;</li> <li>e. Other indirect identifiers, such as the student's date of birth, place of birth, and Mother's Maiden Name;</li> </ul> <p>Examples of staff APPR PII:</p> <ul style="list-style-type: none"> <li>a. Teacher Id, Social Security Number, Employee Number, Biometric Record</li> <li>b. Name, Mother's Maiden Name, Parent's Name</li> <li>c. Birthdate, Place of Birth, Address</li> <li>d. Gender, Race, Salary</li> </ul> <p><input type="checkbox"/> IF YOUR ORGANIZATION/SOFTWARE DOES NOT COLLECT PII, CHECK THIS BOX AND SKIP TO THE BOTTOM, SIGN AND SUBMIT.</p> <p>If you collect the PII information above, please complete the remainder of this form.</p>
<b>Description of the purpose(s) for which Contractor will receive/access PII</b>	<p>OPALS library management application's member directory minimally includes (a) student's name (b) parents' or guardian names (c) home address (if needed by the library) ... elementary schools include student grade, homeroom and possibly homeroom teacher and possibly email addresses - Teacher name and assigned library membership number, grade and homeroom...</p> <p>Data is used to manage library resources loans, reserves, returns and to send pertinent notices</p>
<b>Type of PII that Contractor will receive/access</b>	<p>Check all that apply:</p> <p><input checked="" type="checkbox"/> Student PII</p> <p><input checked="" type="checkbox"/> APPR PII</p>

<b>Contract Term</b>	Contract Start Date <u>09/01/2025</u> Contract End Date <u>08/31/2026</u>
<b>Subcontractor Written Agreement Requirement</b>	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 checked="" type="checkbox"/> Contractor will not utilize subcontractors. <input type="checkbox"/> Contractor will utilize subcontractors.
<b>Data Transition and Secure Destruction</b>	Upon expiration or termination of the Contract, Contractor shall: <ul style="list-style-type: none"> <li>• Securely transfer data to EA, or a successor contractor at the EA's option and written discretion, in a format agreed to by the parties.</li> <li>• Securely delete and destroy data.</li> </ul>
<b>Challenges to Data Accuracy</b>	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.
<b>Secure Storage and Data Security</b>	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply) <input type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party. <input checked="" type="checkbox"/> Using Contractor owned and hosted solution <input type="checkbox"/> Other:  Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:  Security is provided on data, application, hosting level, includes physically secure data center, proven firewall protection, intrusion prevention measures - HIPAA compliant. Authorized library staff can specify levels of user security, using passwords and hierarchical assignment of such. Media Flex Inc. limits access to user's PII to authorized staff who receive pertinent PII instruction.
<b>Encryption</b>	Data will be encrypted while in motion and at rest.

## CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

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

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	Security on the data, application, and hosting level. Physically secure data center, firewall protection, intrusion prevention measures <del>HIPAA compliant</del>
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Authorized library staff can specify levels of user security, using passwords and hierarchical assignment. Media Flex Inc. limits access to PII <del>data to trained, authorized staff</del>
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.	MF does not use subcontractors. (MF partners with some RICs hosting the OPALS system ex. ESBOCES, Erie1, BTBOCES, Dutchess, etc.) PII - PII staff are trained to protect PII using NYS resources: <a href="https://www.nysed.gov/data-privacy-security">https://www.nysed.gov/data-privacy-security</a>
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.	MF staff providing support for the OPALS library system, are required to acknowledge and sign an agreement to adhere to NYS PII & FERPA privacy laws.
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.	Please see the attached "Media Flex IT Security Information and Notification Plan" MF uses audit tools such as "Burp Suite Pro" and "Nessus Pro" to detect vulnerabilities and network engineers audit network traffic for attacks and intrusion incidents. Incident reporting will use NYSE incident reporting form.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Securely transfer data to EA, or a successor contractor or securely delete and destroy data.
7	Describe your secure destruction practices and how certification will be provided to the EA.	MF staff will delete PII data from our server(s) and will provide the EA a secure data destruction certificate confirmation.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	MF data security practices are articulated in Edlaw 2D and on the NYSED data security Website: <a href="https://www.nysed.gov/data-privacy-security/laws-regulations-and-guidance">https://www.nysed.gov/data-privacy-security/laws-regulations-and-guidance</a>
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1	Security is provided on data, application, hosting level, includes physically secure data center, proven firewall protection, intrusion <del>protection measures, HIPAA compliant</del>


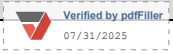
Additional Information:



## Western Suffolk BOCES Education Law §2-d Bill of Rights for Data Privacy and Security

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

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.
2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.
3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.
4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.
5. A complete list of all student data elements collected by NYSED is available at [www.nysed.gov/data-privacy-security/student-data-inventory](http://www.nysed.gov/data-privacy-security/student-data-inventory) and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to: [dpo@wsboces.org](mailto:dpo@wsboces.org). (ii) Complaints may also be submitted to the NYS Education Department at [www.nysed.gov/data-privacy-security/report-improper-disclosure](http://www.nysed.gov/data-privacy-security/report-improper-disclosure), by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to [privacy@nysed.gov](mailto:privacy@nysed.gov); or by telephone at 518-474-0937.
7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.
8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.
9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

CONTRACTOR	
[Signature]	 
[Printed Name]	H. Chan
[Title]	President
Date:	07/31/2025

## **DATA PRIVACY AND SECURITY PLAN**

### **Media Flex Inc.**

Media Flex Inc. maintains a Data Security and Privacy Plan that includes the following elements congruent with New York State Education Law 2-d Rider for Data Privacy and Security:

1. New York State Libraries use OPALS Library Automation software to automate libraries in this region. Only data essential for providing library circulation, online public catalog, and member authentication services are uploaded.
2. Media Flex Inc. does not share, sell, rent or trade Personally Identifiable Information with third parties for promotional purposes on their part. Media Flex Inc. does not upload email addresses without the site visitor voluntarily providing the library with this information.
3. If a library were to terminate its contract with Media Flex Inc., Media Flex Inc. technical support staff would return any library data and destroy any data that might have been stored.
4. To prevent unauthorized access or disclosure, to maintain data accuracy, to allow only the appropriate exercise of a library's Personal Information while also protecting the confidentiality, integrity, and availability of user's Personal Information, Media Flex Inc. employs a variety of industry standard security technologies.
5. An outline of these security technologies is as follows:
  - Security is provided on the data, application, and hosting level to include a physically secure data center, proven firewall protection, and intrusion prevention measures which are HIPAA compliant.
  - Authorized library staff can specify levels of user security, using passwords and hierarchical assignment of such.
  - Media Flex Inc. limits access to user's Personal Information and data to those persons who have a specific purpose for maintaining and processing such information.
6. Media Flex Inc. employees who have access to user's Personal Information are made aware of their responsibilities to protect the confidentiality, integrity, and availability of that information and have been provided training and instruction on how to do so.
7. Media Flex Inc. does not hire or work with subcontractors
8. Media Flex Inc. technical support and computer engineering staff are cognizant of and trained to detect and diagnose as well as notify all parties with respect to security incidents. The Media Flex Inc. Data Breach and Notification Plan is appended.



Harry Chan  
President

Media Flex Inc. - P.O. Box 1107 - Champlain, NY 12919

## Media Flex IT Security Information and Notification Plan

**Incident Handler:** Media Flex Inc. technology security staff

**System Administrator:** Media Flex Inc. “First Responder”

**System Owner:** Context relevant (Could be Media Flex Inc. staff if hosted by MF... or client)

**HIPPA Privacy & Security Officer:** Media Flex Inc. security staff

### **Identification**

**Identify a potential incident:** Incident handler monitors of security sensors. System owners or system administrators do so by observing suspicious system anomalies. Anyone in the library community may identify a potential security incident through external complaint notification.

**Notify:** Library community staff that suspect an IT system has been accessed without authorization must immediately report the situation to [ctho@mediaflex.net](mailto:ctho@mediaflex.net). As soon as the incident handler is aware of a potential incident, s/he will alert local system administrators.

**Quarantine:** The incident handler will quarantine compromised hosts when notified unless they are on a Quarantine Whitelist. If they are on a Quarantine Whitelist, the incident handler will contact the system administrator or system owner to contain the incident. Note that the incident handler alert parties of suspicious behavior when not confident of an incident; in these cases do not quarantine the host immediately, but wait 24-48 hours and quarantine only if the registered contact is unresponsive.

### **Verification**

**Classify:** Critical Incident Response (CIR) procedures when...

1. The system owner or system administrator indicates that the system is a high-criticality asset
2. OR the system owner or system administrator alerts that the system contains Restricted Data
3. OR library staff determines that the system poses a unique risk warranting investigation.

**Verify:** The CIR process should be initiated when...

The incident handler verifies that the alert is not a false positive. The incident handler will double-check the triggering alert, and correlate it against other alerting systems when possible.

AND the type of data or system at risk is verified to be of an appropriate classification, as determined above. The system owner or system administrator should provide a detailed description of the data at risk, including approximate numbers of unique data elements at risk, and the number, location, and type of files it is stored in.

For the CIR process to be initiated the criticality of the asset must be confirmed, and it must be confirmed that the triggering event is not a false positive. In cases where the CIR process is not required, the incident handler can resolve the case as follows:

Obtain a written statement from the system owner or system administrator documenting that the system has no Restricted Data and is not a high-criticality asset.

Obtain a written statement from the system owner or system administrator that the system has been reinstalled or otherwise effectively remediated before quarantine is lifted.

For incidents involving an unauthorized wireless access point, obtain a written statement that the access point has been disabled.

## **Containment**

1. If the host cannot immediately be removed from the network, the incident handler will **initiate a full-content network dump** to monitor the attacker's activities and to determine whether interesting data is leaking during the investigation.
2. **Eliminate attacker access:** Whenever possible, this is done via the incident handler performing network quarantine at the time of detection AND by the system administrator unplugging the network cable. In rare cases, the incident handler may request that network operations staff implement a port-block to eliminate attacker access. In cases where the impact of system downtime is very high, the incident handler will work with system administrators to determine the level of attacker privilege and eliminate their access safely.
3. The incident handler will collect data from system administrators in order to quickly **assess the scope of the incident**, including:
  1. Preliminary list of compromised systems
  2. Preliminary list of storage media that may contain evidence
  3. Preliminary attack timeline based on initially available evidence
4. **Preserve forensic evidence:**
  1. System administrators will capture **first responder data** if the system is turned on. The incident handler will provide instructions for capturing this data to the individual performing that task.
  2. The incident handler will capture disk images for all media that are suspected of containing evidence, including external hard drives and flash drives.
  3. The incident handler will dump network flow data and other sensor data for the system.
  4. The incident handler will create an **analysis plan to guide** the investigation.

The actions that need to be taken will depend on the uptime requirements of the compromised system, the suspected level of attacker privilege, the nature and quantity of data at risk, and the suspected profile of the attacker. The most important goals of this phase are to eliminate attacker access to the system(s) as quickly as possible and to preserve evidence for later analysis.

Additionally, this is the phase where the incident handler works most closely with system administrators and system owners. During this phase they are expected to take instruction from the incident handler and perform on-site activities such as attacker containment, and gathering first response data.

## **Analysis**

The analysis phase is where in-depth investigation of the available network-based and host-based evidence occurs. The primary goal of analysis is to establish whether there is reasonable belief that the attacker(s) successfully accessed Restricted Data on the compromised system. Secondary goals are to generate an attack timeline and ascertain the attackers' actions. All analysis steps are primarily driven by the incident handler, who coordinates communications between other stakeholders, including system owners, system administrators, and

relevant compliance officers. Questions which are relevant to making a determination about whether data was accessed without authorization include:

1. **Suspicious Network Traffic:** Is there any suspicious or unaccounted for network traffic that may indicate data exfiltration occurred?
2. **Attacker Access to Data:** Did attackers have privileges to access the data or was the data encrypted in a way that would have prevented reading?
3. **Evidence that Data was Accessed:** Are file access audit logs available or are file system mactimes intact that show whether the files have been accessed post-compromise?
4. **Length of Compromise:** How long was the host compromised and online?
5. **Method of Attack:** Was a human involved in executing the attack or was an automated "drive-by" attack suite employed? Did the tools found have capabilities useful in finding or exfiltrating data?
6. **Attacker Profile:** Is there any indication that the attackers were data-thieves or motivated by different goals?

Using these factors, the security officer will determine the degree of technical probability that the security or privacy has been compromised. Document each impermissible use and disclosure and the risk assessment conducted for each. That HIPAA Officer will be responsible for conducting the risk assessment, documenting the results of the assessment and whether the impermissible use or disclosure poses a significant risk of financial, reputational or other harm to the individual whose data was compromised.

## **Recovery**

The primary goal of the recovery phase is to restore the compromised host to its normal function in a safe manner.

The system administrators will remediate the immediate compromise and restore the host to normal function.

The system administrators will make short-term system, application, and business process changes to prevent further compromise and reduce operating risk.

## **Reporting**

The final report serves two main purposes. First, a recommendation is made as to whether the incident handler and the responsible officials feel there is a reasonable belief that Data was disclosed impermissibly without authorization and the degree of probability that security or privacy has been compromised. The report will be made to allow notification, if appropriate, within any legally-mandated time period. In the case of HIPAA/HITECH/Omnibus, that is within 60 days of discovering the Breach. Second, a series of mid-term and long-term recommendations will be made to the owners of the compromised system, including responsible management, suggesting improvements in technology or business process that could reduce operating risk in the future.

1. The incident handler will draft the final report after the investigation is complete.
2. After the draft report is completed, signoff on the content of the report should be obtained from management. Technical personnel can offer comments as well.
3. For critical incidents involving payment card data, the PCI Compliance Manager will receive a copy of the report and appropriate entities will be notified in the event that cardholder data is accessed without authorization. The Compliance Manager will be responsible for all communication with the payment



card brands and will be responsible for coordinating the activities mandated by the payment card brands with respect to the incident.

4. For critical incidents, the report will include each impermissible use and disclosure and the risk assessment conducted for each.
5. The incident handler will schedule a meeting to deliver the final report to the system administrator and the system owner.
6. The incident handler will ensure that the final report includes the details of the investigation and mid-term and long-term recommendations to improve the security posture of the organization and limit the risk of a similar incident occurring in the future.

### **Data Retention**

1. The incident handler will archive the final report in case it is needed for reference in the future; reports must be retained for six (6) years.
2. Incident notes should be retained for six (6) months from the date that the report is issued. This includes the investigation page, file-timelines and filtered network-flows.
3. Raw incident data should be retained for thirty (30) days from the date that the report is issued. This includes disk-images, unfiltered netflow-content, raw file-timelines, and other data that was collected but deemed not relevant to the investigation.

03/20/2025