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.

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 though 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 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 2448 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 fullcontent 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 portblock 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 HIPPA 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 midterm 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.

04/05/2017