

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).

Name of Contractor	
Description of the purpose(s) for which Contractor will receive/access PII	
Type of PII that Contractor will receive/access	Check all that apply: <input type="checkbox"/> Student PII <input type="checkbox"/> APPR Data
Contract Term	Contract Start Date _____ Contract End Date _____
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="checkbox"/> Contractor will not utilize subcontractors. <input type="checkbox"/> Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: <ul style="list-style-type: none"> 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. Securely delete and destroy data.
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 Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.

Secure Storage and Data Security	<p>Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply)</p> <p><input type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party.</p> <p><input type="checkbox"/> Using Contractor owned and hosted solution</p> <p><input type="checkbox"/> Other:</p> <p>Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:</p>
Encryption	<p>Data will be encrypted while in motion and at rest.</p>


CONTRACTOR	
Signature:	
Printed Name:	
Title:	
Date:	

EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

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.	
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 using the Framework chart below.	PLEASE USE TEMPLATE BELOW.

EXHIBIT C.1 – NIST CSF TABLE

The table below will aid the review of a Contractor's Data Privacy and Security Plan. Contractors should complete the Contractor Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. To complete these 23 sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-7 ; (ii) Use a narrative to explain alignment (may reference its applicable policies); and/or (iii) Explain why a certain category may not apply to the transaction contemplated. Further informational references for each category can be found on the NIST website at <https://www.nist.gov/cyberframework/new-framework>. Please use additional pages if needed.

Function	Category	Contractor Response
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	Policies, processes, and procedures around asset management generally follow the direction set by the Corporate Security Policy and are managed consistently with their relative importance to organizational objectives. We are working towards the implementation of a high-level risk strategy in upcoming years.
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	Policies, processes, and procedures generally follow the direction set by the Corporate Security Policy in these areas.
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	Policies, processes, and procedures generally follow the direction set by the Corporate Security Policy in these areas.
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Policies, processes, and procedures around risk management generally follow the direction set by the Corporate Security Policy and are managed consistently with their relative importance to organizational objectives. We are working towards the implementation of a high-level risk strategy in upcoming years.
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Policies, processes, and procedures around risk management generally follow the direction set by the Corporate Security Policy and are managed consistently with their relative importance to organizational objectives. We are working

Function	Category	Contractor Response
		towards the implementation of a high-level risk strategy in upcoming years.
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	The organization reviews and mitigates supply chain risks on a regular basis.
PROTECT (PR)	Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	Active Directory and Multi-factor authentication is used to access backend end system. Web user access is controlled using local authentication. Industry best practices are used for password strength.
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	Security training and acknowledgement of our corporate information security policy is required for all staff and contractors annually and immediately upon hire.
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	All connections are transmitted over secure channels using strong encryption (TLS 1.2). persistent data stored (at rest) is encrypted within our Microsoft Azure Cloud services. Systems and data are managed in a way that is consistent with our corporate information security policy.
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	Policies, processes, and procedures generally follow the direction set by the Corporate Security Policy in these areas. For instance, access is granted using a least-privilege model based on need. Where resources permit, access is granted based on defined roles and separation of duties.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	Automated Backups are conducted regularly. Maintenance and repairs of the physical components are managed by Microsoft within the Azure Cloud.
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	Technical tools used are consistent with our policies, procedures, and agreements. For instance, tools such Web vulnerability scanners are deployed to identify potential risks and guide remediation efforts.

Function	Category	Contractor Response
DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	Azure PaaS services provides infrastructure Anomaly and Event management features via Microsoft Defender for App Services.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	Azure PaaS services provides infrastructure Anomaly and Event management features via Microsoft Defender for App Services.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Azure PaaS services provides infrastructure Anomaly and Event management features via Microsoft Defender for App Services.
RESPOND (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	Incidents are managed in a way that is consistent with our corporate information security policy and incident response process.
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	Our incident response procedures call for this type of communications.
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	Our incident response procedures call for this type of activity.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Our incident response procedures call for this type of activity.
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	We continually assess and enhance our processes to address the evolving threat environment as time and resources permit.
RECOVER (RC)	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	Restoration of application and database assets are done using routinely taken backups in accordance with our incident response procedures.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	Our incident response procedures call for this type of activity. Additionally, retrospectives are routinely conducted to discussion process improvements.
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	Our incident response procedures call for this type of activity. Internal and external communication is done on a case-by-case basis.

EXHIBIT "D" FROM VENDOR - ZANER-BLOSER, INC.

PRIVACY POLICY

Zaner Bloser, Inc. ("Zaner-Bloser", "we", "us") respects your privacy and is committed to protecting it through our compliance with this policy.

This policy was last updated on June 29, 2020.

For your convenience, here is our contact information:

Our postal address is

PO Box 16764

Columbus, OH 43216-6764

Our address is

1400 Goodale Boulevard, suite 200

Grandview Heights, OH 43212

We can be reached via e-mail at customerexperience@zaner-bloser.com or you can reach us by telephone at [1-800-421-3018](tel:1-800-421-3018).

ZANER-BLOSER.COM AND SHOP.ZANER-BLOSER.COM

What We Collect and How to Opt-Out

Domain Name and E-Mail Address:

For each visitor to our website, our web server automatically recognizes the visitor's domain name and e-mail address (where possible). We collect the domain name and e-mail address (where possible) of visitors to our website, the e-mail addresses of those who post messages to our bulletin board, the e-mail addresses of those who communicate with us via e-mail, aggregate information on what pages our visitors access or visit, information volunteered by the visitor such as survey information and/or site registrations, and referring pages. If you do not want to receive e-mail from us in the future, please follow the opt-out process in the e-mail or contact us through one of the methods listed above.

Postal Information:

If you supply us with your postal address online, you may receive periodic mailings from us with information on new products and services or upcoming events. If you do not wish to receive such mailings, please let us know by sending e-mail to us at the above address, calling us at the above telephone number, or writing to us at the above address.

Telephone Information:

Persons who supply us with their telephone numbers online may receive telephone contact from us with information regarding orders they have placed online. They also may receive telephone contact from us with information regarding new products and services or upcoming events. If you do not wish to receive such telephone calls, please let us know by sending e-mail to us at the above address, calling us at the above telephone number, or writing to us at the above address.

Online Orders:

Persons who place online orders with us provide information to us via an online order form that is used to fulfill the order, to contact the customer if necessary, and to market our programs. Credit card and other financial information collected by our third party payment processor are used to bill the customer for products and services.

Cookies:

We use cookies to record session information, such as items that customers add to their shopping cart. Our customers can choose to have "Remember Me" information recorded in our database so that when they return, their information will be retrieved. We may also use cookies for the purpose of re-targeting ads to you. Based on the products or information you view on our website, you may see information about our products for a limited period of time on your future visits to the internet. If you do not want to see these ads, simply click on this [Opt-Out Link](#). In addition, your computer can be configured to delete cookies or to disable them altogether, but note that you may not be able to use some of the services available on our website as a result. The information that we collect and share in this fashion is de-identified, does not contain personally identifiable information, and is intended for advertising to people over the age of 13.

How We Use and Disclose the Information We Collect:

In addition to the uses described above, the information we collect is used

- to improve the content of our website.
- to notify you about updates to our website.
- to carry out our obligations and enforce our rights arising from any contracts entered into between you and us, including for billing and collection.
- to contact you for marketing purposes.
- in any other way we may describe when you provide the information.
- for any other purpose with your consent.

We may disclose information that we collect or you provide as described in this privacy policy

- to our subsidiaries and affiliates, including the members of the Highlights Family of Companies.
- to contractors, service providers, and other third parties we use to support our business, such as our third party payment card processor.
- to a buyer or other successor in the event of a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of Zaner-Bloser's assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which information held by us about our website visitors is among the assets transferred.

New Uses of Information:

From time to time, we may use visitor information for new, unanticipated uses not previously disclosed in our privacy policy. If our information practices change at some time in the future, we will post the policy changes to our website to notify you of these changes. If you are concerned about how your information is used, you should visit our website periodically and review our policies.

Access to Your Information:

Upon request, we provide visitors with access to their transaction information. You can make such a request by contacting us through one of the methods listed above.

Correction of Your Information:

If you notice any inaccuracies in your transaction information, you may contact us through one of the methods listed above and we will work with you to make any corrections deemed necessary. We may not accommodate a request to change information if we believe the change would violate any law or legal requirement or cause the information to be incorrect.

Your California Privacy Rights:

California Civil Code Section § 1798.83 permits users of our website who are California residents to request certain information regarding our disclosure of personal information to third parties for their direct marketing purposes. To make such a request, please email or write to us at the contact information provided above.

Third-Party Web Sites:

This site contains links to other websites. Zaner-Bloser is not responsible for the privacy practices or the content of such websites.

Data Security:

We have implemented measures designed to secure your information from accidental loss and from unauthorized access, use, alteration, and disclosure.

The safety and security of your information also depends on you. Where we have given you (or where you have chosen) a password for access to certain parts of our website, you are responsible for keeping this password confidential. We ask you not to share your password with anyone.

Unfortunately, the transmission of information via the internet is not completely secure. Although we do our best to protect your personal information, we cannot guarantee the security of your personal information transmitted to our website. Any transmission of personal information is at your own risk. We are not responsible for circumvention of any privacy settings or security measures contained on the website.

CALIFORNIA RESIDENT SUPPLEMENT:

If you are a California resident, the processing of certain personal data about you may be subject to the California Consumer Privacy Act ("CCPA") and other applicable California state privacy laws. Beginning

January 1, 2020, the CCPA gives you certain rights with respect to the processing of your personal data (known as “personal information”, as described in under the CCPA).

This supplement provides additional privacy disclosures and informs you of your additional rights as a California resident, and should be read in conjunction with our Privacy Policy as set forth above.

Personal Information Collected and Processed

Our Privacy Policy sets forth the categories of personal information that Zaner-Bloser collects and processes about you, a description of each category, and the sources from which we obtain each category.

Requests to Exercise Your Rights

RIGHT TO KNOW REQUEST - Under the CCPA, you have a right to request information about our collection, use, and disclosure of your personal information over the prior 12 months, and ask that we provide you with the following information:

1. Categories of and specific pieces of personal information we have collected about you.
2. Categories of sources from which we collect personal information.
3. Purposes for collecting, using, or selling personal information.
4. Categories of third parties with which we share personal information.
5. Categories of personal information disclosed about you for a business purpose.
6. If applicable, categories of personal information sold about you and the categories of third parties to which the personal information was sold, by category or categories of personal information for each third party to which the personal information was sold.

To make a verifiable request for information about the personal information we have collected about you, please contact us via e-mail at customerexperience@zaner-bloser.com or you can reach us by telephone at 1-800-421-3018.

RIGHT TO DELETE REQUEST - You also have a right to request that we delete personal information, subject to certain exceptions. You may exercise your right to delete by using contacting us via email at customerexperience@zaner-bloser.com or you can reach us by telephone at 1-800-421-3018.

REQUESTS, GENERALLY - Please note, if you do not have a Zaner-Bloser account we will not have enough information about you to verify your Right to Know and Right to Delete requests, as we do not keep sufficient information necessary to reidentify and link you to a prior visit to zaner-bloser.com where data may have been collected. As such, we will be unable to verify and honor your requests. You may make a verifiable consumer request related to your personal information twice per 12-month period. We will not discriminate against you for exercising any of your rights under the CCPA.

REQUESTS MADE THROUGH AGENTS - You may designate, in writing or through a power of attorney, an authorized agent to make requests on your behalf to exercise your rights. Before accepting such a

request from an agent, we will require the agent to provide proof you have authorized it to act on your behalf, and we may need you to verify your identity directly with us.

MYZBPORTAL.COM and SUPERKIDS PORTAL

Please be advised that there are important differences in how Zaner-Bloser handles data in connection with the MYZBPORTAL and the SUPERKIDS Portal, specifically in connection with any data that may include Student PII (Personally Identifiable Information).

School data and PII:

MyZBPortal.com and the Superkids Portal (“Portal”) collect the following student PII:

- Student first name (provided by district/school/institution)
- Student last name (provided by district/school/institution)
- Student ID (provided by district/school/institution)
- IP address
- Student score data (from completing online activities)

We only collect IP addresses for traffic and security monitoring purposes and delete these logs regularly (typically every other month). Schools can also request to delete these IP logs by submitting a request in writing to ZB Customer Experience.

- We do not sell student information.
- We do not target students with advertisements.
- We only request and use student personal information for legitimate business reasons.

Cookies:

Superkids Portal (Teachers, Admins, Parents) and Superkids Online Fun app and desktop shortcut (Students)

The entire site maintains cookies from the moment you visit the login page. The sole purpose of the use of cookies on the Superkids Portal is to track the user’s session and visit. Zaner-Bloser, Inc.’s use of cookies is specifically limited to the legitimate business use for operation of the portal and cookies are never used for any targeted advertisements toward students.

ZB Portal (Teachers, Admins, Students)

The entire site maintains cookies from the moment you visit the login page. The sole purpose of the use of cookies on the MYZBPortal is to track the user’s session and visit. Zaner-Bloser, Inc.’s use of cookies is specifically limited to the legitimate business use for operation of the portal and cookies are never used for any targeted advertisements toward students.

Data encryption:

Stored data (i.e. data at rest) is stored securely on an encrypted drive. Data on backup storage is encrypted using AES 256-bit encryption. Data 'in-transit' is encrypted using well-known technologies such as "Secure Sockets Layer (SSL)" or "Transport Layer Security (TLS)". In-transit encryption is end-to-end from the client web browser through our cloud network. These protocols ensure privacy between communicating applications and their users on the Internet. When a server and client communicate, these technologies ensure that no third party may eavesdrop or tamper with any message.

Data retention:

At any time, an account administrator may request to purge school data (such as student and/or teacher information). This action will be performed by a ZB representative. School information will remain on backup storage for disaster recovery purposes for another 15 days, but thereafter will be removed completely from all storage devices. Schools can request to delete school data submitting a request in writing to ZB Customer Experience.

Data access:

Only authorized individuals are provided access to our systems. Passwords are never transmitted using insecure communication protocols. Access by Company's support personnel is based on "least privileged" and "need to know" basis. While some Company support personnel generate usage reports and have access to data for analytics, none of the resultant data contains Personally Identifiable Information (PII).

System hosting:

Our systems (servers and data) are currently hosted on dedicated machines in secured facilities at a third-party hosting provider located in the United States.

Perimeter security:

Firewalls and perimeter detection systems have been designed and deployed to help detect and prevent unauthorized access into our systems.

Vulnerabilities and patching:

We routinely scan our systems for vulnerabilities. The vulnerabilities are reviewed and addressed/patched as appropriate.

Consent from Schools regarding Students' Personal Information:

The Children's Online Privacy Protection Act ("COPPA") permits a school, acting in the role of "parent" to provide required consents regarding personal information of students who are under the age of 13. Where a school is the subscriber to our portal, we rely on this form of COPPA consent. We provide the school with this privacy policy, to ensure that the school, in providing its COPPA consent, has full information and assurance that our policies comply with COPPA.

The Family Educational Rights and Privacy Act ("FERPA") permits a school to provide educational records

(including those that contain students' personal information) to certain service providers without requiring the school to obtain specific parental consent. FERPA permits this where the service provider acts as a type of "school official" by performing services, for example, that would otherwise be performed by the school's own employees. We fulfill FERPA requirements for qualifying as a school official by, among other steps, giving the school direct control with respect to the use and maintenance of the education records at issue (including associated personal information), and refraining from re-disclosing or using this personal information except for the purposes of providing this portal to the school. We comply with FERPA by relying on this form of consent.

Your Rights:

As a user of the portal, you have the rights to access, export, be informed about, rectify, object to the further processing of, restrict the processing of, withdraw consent to the processing of and erase your personal information. If you are a student at an educational institution using the Portal, you should direct any requests to exercise your data rights to the appropriate representative at your educational institution. If you are an educator or an administrator, you may reach out to us directly via e-mail at customerexperience@zaner-bloser.com or you can reach us by telephone at 1-800-421-3018.

School data and PII:

MyZBPortal.com collects the following student PII (personally identifiable information):

- Student first name (provided by district/school/institution)
- Student last name (provided by district/school/institution)
- Student ID (provided by district/school/institution)
- IP address
- Student score data (from completing online activities)

We only collect IP addresses for traffic and security monitoring purposes and delete these logs regularly (typically every other month). Schools can also request to delete these IP logs by submitting a request in writing to ZB Customer Experience.

- We do not sell student information.
- We do not target students with advertisements.
- We only request and use student personal information for legitimate business reasons.

Data encryption:

Stored data (i.e. data at rest) is stored securely on an encrypted drive. Data on backup storage is encrypted using AES 256-bit encryption. Data 'in-transit' is encrypted using well-known technologies such as "Secure Sockets Layer (SSL)" or "Transport Layer Security (TLS)". In-transit encryption is end-to-end from the client web browser through our cloud network. These protocols ensure privacy between communicating applications and their users on the Internet. When a server and client communicate, these technologies ensure that no third party may eavesdrop or tamper with any message.

Data retention:

At any time, an account administrator may request to purge school data (such as student and/or teacher information). This action will be performed by a ZB representative. School information will remain on backup storage for disaster recovery purposes for another 15 days, but thereafter will be removed completely from all storage devices. Schools can request to delete school data submitting a request in writing to ZB Customer Experience.

Data access:

Only authorized individuals are provided access to our systems. A username and password must be input and authenticated prior to gaining access to any information. Passwords use one-way salted hashes and technical support does not have access to a user's password. Passwords are **never** transmitted using insecure communication protocols. Access by Company's support personnel is based on "least privileged" and "need to know" basis. While some Company support personnel generate usage reports and have access to data for analytics, none of the resultant data contains Personally Identifiable Information (PII).

System hosting:

Our systems (servers and data) are currently hosted on dedicated machines in secured facilities at a third-party hosting provider located in the United States.

Perimeter security:

Firewalls and perimeter detection systems have been designed and deployed to help detect and prevent unauthorized access into our systems.

Vulnerabilities and patching:

We routinely scan our systems for vulnerabilities. The vulnerabilities are reviewed and addressed/patched as appropriate.

Zaner-Bloser, Inc. Security Incident Response Process

The following denotes the high-level steps to be followed when a potential security issue is suspected, reported, or detected. In case of an actual *security incident*, detailed procedures for each of the steps will be carried out based upon the type and/or nature of the incident.

Assessment

- Assess the potential security issue and all pertinent information to determine if the event is an actual security incident.

Note: This process will stop here if it is determined that the reported issue was not an actual security incident and no breach occurred

- Determine if any *Cardholder Data* is involved
- Create a Security Incident Report Form and document the preliminary findings
- Notify (via email) SIRT at: SIRT@highlights.com and the Information Security Steering committee (ISSC) at: ISSC@Highlights.com that an actual security incident has occurred
- If necessary, notify the user(s) of the affected device, system or network that a problem has occurred and access and/or usage must be limited and/or halted until the problem is resolved
- Document ongoing analysis as appropriate on the Security Incident Response Form

Containment

- If *Cardholder Data* (CHD) is involved:
 - Do not access or alter compromised system(s) (e.g., do not log on to the compromised system(s) and change passwords; do not log in with administrative credentials). The compromised system(s) must be taken offline immediately and not be used to process payments or interface with payment processing systems.
 - Do not turn off, restart, or reboot the compromised system(s). Instead, isolate the compromised systems(s) from the rest of the network by unplugging the network cable(s) or through other means.
 - Preserve all evidence and logs (e.g. original evidence such as forensic image of systems and malware, security events, web logs, database logs, firewall logs, etc.).
 - Await further instruction from the ISSC or the V.P., Government Relations, Information Security and Privacy before proceeding with this process
- If *Cardholder Data* (CHD) is not involved:
 - Determine if it is necessary to disconnect the device from the Internet and/or the network
 - Determine if it is necessary to shut down the affected device, system, or network

- Preserve all evidence and logs (e.g. original evidence such as forensic image of systems and malware, security events, web logs, database logs, firewall logs, etc.).
- Document and track all actions taken to contain the *security incident* on the Security Incident Response Form

Eradication

- Eradicate the problem that is affecting the device, system or network
- Determine whether disk drives should be cleaned/reformatted
- Ensure that previous device, system, and/or network file backups are not infected and take appropriate action
- Document and track all actions taken to eradicate all issues related to the security incident on the Security Incident Response Form

Restoration

- Decide whether the device, system and/or network needs to be restored from previous uninfected file backups
- Perform recovery procedures/processes as required
- Document and track all actions taken to restore workstation, network, system, etc. to its normal state on the Security Incident Response Form

Communication and Notification

- Communicate the appropriate information to the appropriate senior management personnel regarding the occurrence of the security incident (if a breach occurred)
- As warranted, notify the appropriate external entities (law enforcement, federal agency, state agency, Office of the Privacy Commissioner of Canada, payment card brands, payment card acquirers, customers, etc.) regarding the occurrence of the security incident (if a breach occurred involving credit card information or other personally identifiable information)
- If a user's workstation has to be reimaged due to a security incident, the user's manager will be notified and a copy of the Security Incident Response Form sent to the manager

Closure

- Ensure that the incident response process and the Cardholder Data Security Breach Response Process is updated with all lessons-learned and all appropriate industry developments regarding security incident or security breach response
- Ensure that all documentation, data, and/or information related to the security incident has been captured and is securely stored
- Ensure that all appropriate internal and external communication has been conducted as required