Joint Board Meeting
July 13, 2020

Approval Item: Approve the revised ORCA Incident Response Plan

Purpose: This plan provides security incident coordination between the agencies and guidance to identify and respond to ORCA security incidents or breaches, including procedures to manage and prevent breaches.

Background: The original ORCA Breach Plan was adopted by the Joint Board on January 11, 2010, pursuant to Exhibit H, Section 2.3.3, of the Interlocal Agreement. The Plan was revised in its entirety in October 2014 with additional revisions approved in September 2015.

The revised Plan includes updates to reflect current processes and terminology, and replaces the September 2015 version in its entirety.

Recommendation: The Regional Security Engineer and Site Managers recommend approval of the revised ORCA Incident Response Plan.

ORCA Incident Response Plan

July 13, 2020

This content replaces the Plan adopted 2015-09-14 in its entirety

1.0 PURPOSE

This ORCA Incident Response Plan is prepared pursuant to Exhibit H Section 2.3.3 of the Amended and Restated Interlocal Cooperation Agreement for Design, Implementation, Operation and Maintenance of the Regional Fare Coordination System, dated April 14, 2009, ("Interlocal Agreement") which requires Security Incident coordination between the Agencies and within policies approved by the Joint Board.

2.0 SCOPE OF PLAN

The ORCA Incident Response Plan addresses management of any event that affects system security, including those related to credit card transactions and Personally Identifiable Information (PII) for the ORCA system. This plan establishes the process for identifying, responding to and managing all information for security events (including incidents and breaches), and provides for coordination of response activities between the agencies and the ORCA Contractor.

3.0 DEFINITIONS

3.1 "Agency" means one of the following ORCA agencies: Snohomish County Public Transportation Benefit Area ("Community Transit"), City of Everett ("Everett Transit"), King County ("King County Metro"), Kitsap County Public Transportation Benefit Area ("Kitsap Transit"), Pierce County Public Transportation Benefit Area Corporation ("Pierce Transit"), Central Puget Sound Regional Transit Authority ("Sound Transit"), and Washington State Department of Transportation ("Washington State Ferries").

3.2 "Agency Security Representative" (ASR) means the person designated by each participating agency to manage and document security procedures as well as report any security events. This person may designate an agency representative to coordinate an agency-specific security events.

3.3 "Contractor" or "ORCA Contractor" means Vix Technology USA, or its successors or assigns that are under contract with the agencies to operate and maintain the ORCA system.

3.4 "Emergency and Security Breach Contacts" means the roster of Agency and Contractor contacts to be used for notification during any security events.

3.5 "Incident Commander" (IC) means the Regional Security Engineer or a person acknowledged or assigned by the RSE, who, during a declared Security Incident, is authorized to manage the operational aspects of a Security Incident, establish delegation of authority, and elicit advice as needed from the Regional Program Administrator and Operations Manager or ORCA Contractor to determine the nature and scope of an incident. This may be the Regional Security Engineer (RSE), Information Security Officer (ISO), Agency Security Representative (ASR), or a person designated by the RSE.

3.6 "Information Security Officer" (ISO) means the Contractor staff responsible for monitoring and analyzing the ORCA system to detect security flaws and vulnerabilities and to work with the Regional Security Engineer to report and resolve security events, incidents or breaches. The ISO or designated Contractor representative may serve as the authorized Incident Commander (IC).

3.7 "Notice-Triggering Information" requires, as provided in Washington State RCW (RCW) 42.56.590, immediate notice to individuals when a breach of security involves unencrypted, computerized "Personally Identifying Information". NOTE: Per RCW 42.56.590(3) notifications may be delayed if law enforcement determines notification will impede a criminal investigation.

3.8 "ORCA Chief Information Security Officer" (CISO) means the employee of the Regional Program Administration Agency who reports to the Joint Board and who performs the functions of this position under the ORCA Security Committee Charter. The CISO may also serve as the authorized Incident Commander (IC).

3.9 "ORCA Operations Manager" means the person designated by the Joint Board who performs the duties of the ORCA Operations Manager under the Interlocal Agreement.

3.10 "ORCA Security Committee" (OSEC) means the committee established by the Joint Board under the ORCA Security Committee Charter to ensure a coordinated approach to standard and emergency system security procedures throughout the region.

3.11 "Personally Identifying Information" (PII) means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

3.12 “Regional Program Administration Agency” means the agency designated by the Joint Board that is responsible for performing the functions under the Interlocal Agreement.

3.13 “Regional Program Administrator” (RPA) means the person designated by the Joint Board who performs or ensures performance of duties of the Regional Program Administration Agency under the Interlocal Agreement.

3.14 “Regional Security Engineer” (RSE) means the employee of the Regional Program Administration Agency who serves as security expert representing the ORCA agencies in the technical evaluation of all proposed actions and activities that may have an impact on the ORCA system. The RSE may serve as the authorized Incident Commander (IC).

3.15 “Security Breach” means an incident or event that has escalated to the point where a risk has been exploited.

3.16 “Security Event” means any event in the system that can escalate to an incident or a breach, but is not currently putting the system in direct danger.

3.17 “Security Incident” means an event that compromises or has the potential to compromise the confidentiality, integrity or availability of an agency’s or contractor’s information system(s) or data assets. Security events may be declared as security incidents by Agency, Contractor or regional security personnel (see below). A Security Incident may include but is not limited to any or all of the following:

- A violation of an Agency’s or Contractor’s information systems’ security policies and standards.
- Unauthorized computer or data access.
- Presence of mobile code, such as a virus, Trojan, worm etc., zero day threat.
- Presence of unexpected or unusual programs.
- A denial of service (DoS) condition against data, network or ORCA information systems (including distributed denial of service DDoS).
- Misuse of a service, systems or information.
- Physical or logical damage to systems (physical is out of scope for this standard).
- Computer theft.
- Device theft.

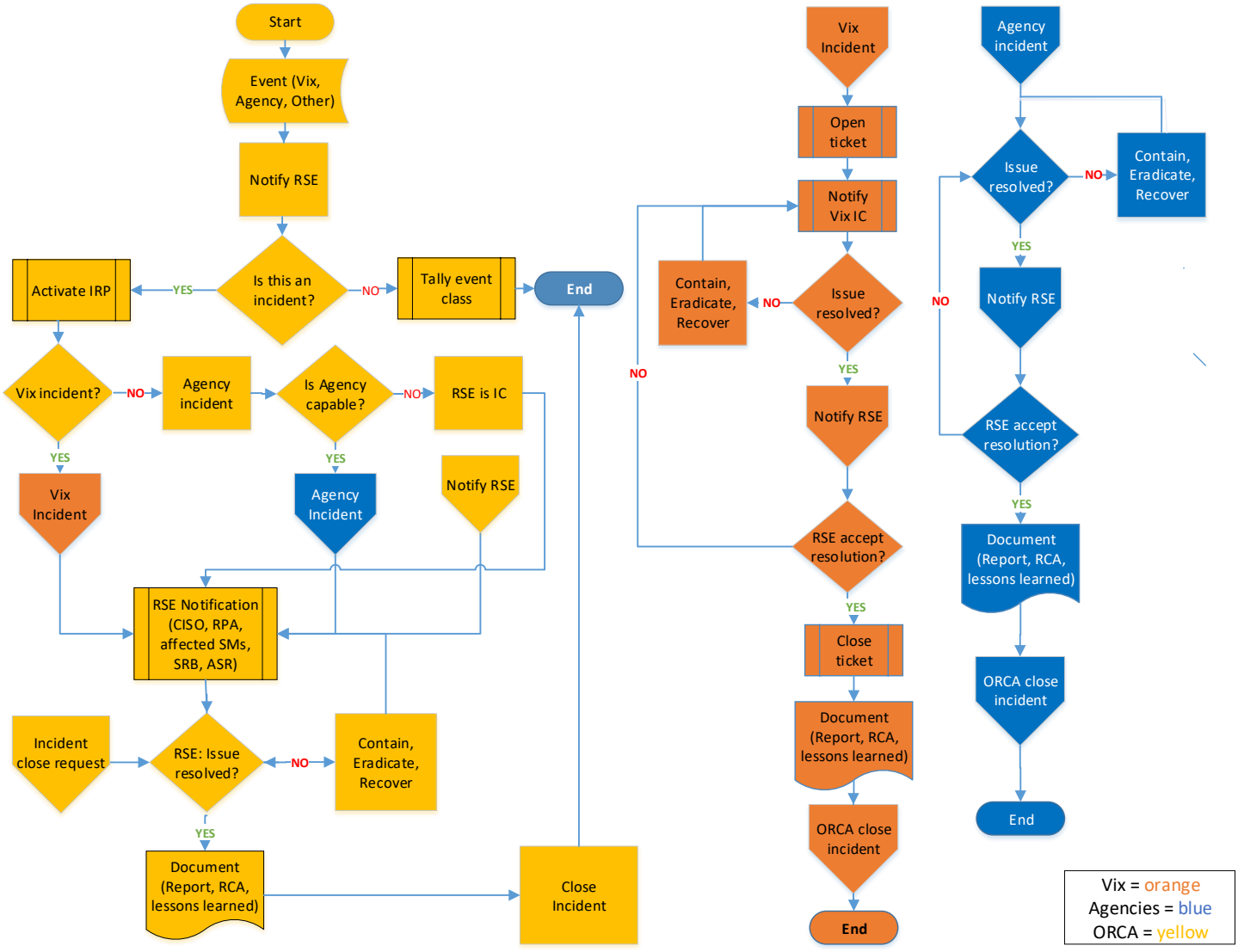
3.18 “Security Review Board” (SRB) means the organization formed under the Contract to address and identify a security compliance strategy. The SRB includes ISO, OSEC and RPA representatives.

3.19 “Site Manager” (SM) means the person designated by an Agency to act as their primary point of contact and the person authorized to speak for that Agency in matters defined under the Interlocal Agreement.

4.0 INFORMATION SECURITY INCIDENT MANAGEMENT – OVERVIEW Table updates pending

This document follows the incident response process diagram below. The process covers the seven phases of the Incident Response Process (IRP):

1. Detection
2. Analysis
3. Triage
4. Escalation
5. Containment and Eradication
6. Recovery
7. Post incident or root cause analysis (RCA).



4.1 Event Detection

4.1.1 When an event is observed, and reported to the Regional Security Engineer (RSE), the RSE will perform a preliminary risk assessment and determines if further investigation is required. Where warranted, a Security Incident will be declared (see Section 4.4).

4.1.2 If an event is received from an individual Agency or a Contractor that they deem to be an incident, the RSE then declares a Security Incident, identifies the Incident Commander (IC), and proceeds accordingly.

4.1.3 The Agencies or the Contractor should report a Security Event to the RSE as soon as possible but no later than 8 hours from the time initially detected.

4.2 Event Analysis

As the types of events are varied, the analysis phase consists of various information gathering techniques in order to ensure the data is accurate and valid. During this phase, the goal is to determine if the event has contextual impact to the Agencies, Contractor or customer base, and if more evaluation is needed. If more evaluation is required, the event will be defined as an incident and continued analysis will occur.

4.3 Incident Detection

4.3.1 The incident detection phase involves observation of malicious or anomalous activity (initially known as a “Security Event”) gathering of information that provides insight into security threats or risks to ORCA information systems. Reports of security events from sources external to ORCA (contractor or agency, etc.) may also trigger a Security Event.

4.3.2 Incident detection involves (but is not limited to) the use of intrusion detection systems (IDS & IPS), endpoint security applications, network monitoring and web application firewalls. Security news alerts, communications from vendors, reports from employees or customers may also trigger a Security Event.

4.3.3 The Agencies or the Contractor should report a Security Incident to the RSE as soon as possible but no later than 8 hours from the time initially detected.

4.4 Incident Declaration

If an event is determined to affect the confidentiality, integrity or availability of regional systems, the RSE will declare a regional Security Incident. Communication and coordination between the RSE and IC, regardless of where the incident occurs, is crucial to addressing the incident. During all incidents, the RSE and IC will be in constant, regular contact. The frequency of this contact will change over the course of the incident, but will remain until the incident is closed.

4.5 Breach Declaration

If investigation of an event determines unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person or entity, the Regional Program Administration Agency will assess what notification to individuals is appropriate under RCW 19.255.010 and 42.56.590. See *Appendix E - Breach Response Notification of Card Vendor*.

4.6 Triage

During the triage phase, the IC will review the data collected during the analysis phase to determine the potential impact to confidentiality, integrity or availability of the ORCA system.

4.7 Containment & Eradication

4.7.1 Most incidents require early containment before an incident overwhelms ORCA resources or increases damage. Quick, but thorough, decision making (e.g., shut down a system, disconnect it from a network, or disable certain functions) helps minimize risk and damage. The Incident Commander will make these decisions as quickly as needed to contain the incident. The IC (Contractor ISO, agency IC, etc.) and RSE may make determinations as to allowing assets and or services to be shut down if deemed necessary during an incident.

In general, shutdown of assets/services will be done by conferring with RPA, ORCA CISO, Agencies, Joint Board, et al. However, some situations may be time sensitive and require urgent decisions between the IC, Contractor and RSE. Under such events, a decision may be taken prior to consultation of the RPA, ORCA CISO or Agencies, but all such entities MUST be advised why that shutdown was warranted and the reasoning behind said actions.

4.7.2 The immediate goal of the containment phase is to prevent further impact from the incident as well as continue investigation to validate it is an ongoing incident. In parallel with containment, the process will preserve evidence, gather information, and mitigate risks associated with the incident.

4.7.3 In the eradication phase, the goal is to discover the origin of the incident, the root cause of the problem and eliminate components of the incident, including removing malware from systems and disabling user accounts.

4.8 Recovery

4.8.1 Recovery is the phase in the process where all impacted systems (assets) are brought back into compliance with their pre-incident configurations. This may include rebuilding assets or engagement of impacted customers as required by compliance needs, or governmental agency directives.

4.8.2 Additionally, during this phase all pertinent notes regarding activities are updated within appropriate information repositories as designated by Incident Commander.

4.8.3 In recovery, administrators restore systems to normal operation and remediate vulnerabilities to prevent similar incidents. Recovery may involve but is not limited to any of the following actions:

- Restoring systems from clean backups
- Rebuilding systems from scratch
- Replacing compromised files with clean versions
- Installing patches
- Changing passwords
- Tightening network perimeter security (e.g., firewall rule sets, boundary router access control lists).

4.8.4 Higher levels of system logging or network monitoring are often part of the recovery process. These actions help prevent continuing attacks available until completion of eradication and recovery. **Note**: Because eradication and recovery actions are typically operating system or application-specific, this document does not cover detailed recommendations and advice.

5.0 INCIDENT RESPONSE

5.1 Notification

The Regional Program Administrator will inform the Joint Board of the incident via e-mail as soon as possible, in coordination with the Regional Security Engineer or Incident Commander.

5.1.1 The Regional Program Administration agency officials, must determine when notification to individuals is appropriate under RCW 42.56.590. Notification is an important part of the mitigation strategy and has the potential to benefit both the agencies and the individuals affected by a breach. Washington law provides specific guidance on steps to take. Consider each incident on a case-by-case basis to determine whether breach notification is required.

5.1.2 In general, ORCA, through the Regional Program Administration Agency, is required to provide notice to any resident of this State whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person following discovery or notification of the breach in security of the data. Refer to RCW 42.56.590 which requires immediate notification be provided to the owner of personal information when a Security Breach of the data occurs.

5.1.3 If it is determined that the breach involved Notice-Triggering Information, the Regional Program Administration Agency will take the appropriate steps. Refer to *Appendix E - Breach Response Notification of Card Vendor*.

5.1.4 If the breach includes credit card data, the RSE or designee will notify law enforcement prior to notifying merchant bank and credit card vendor. Refer to *Appendix E.*

5.1.5 The Security Review Board, Incident Commander and/or Agency Security Representative or Incident, will identify and investigate the incident and lead the evaluation of risk factors. When assessing associated risks, the questions provided by the Incident Commander in *Appendix A - Initial Security Incident Assessment* will be considered.

5.2 Incident Handling Process

Regardless of the origin, all security events need to be communicated to the Regional Security Engineer (RSE). A determination will be made (see below) on who will lead the response activities, based on the evaluation factors such as personnel and/or systems involved, etc. Irrespective of who is assigned to lead response, the only person allowed to close an incident is the RSE. Response actions **must be coordinated by the RSE.** Agency and Contractor staff will follow this initial response protocol when a Security Event occurs:

5.2.1 The Regional Security Engineer—or designee in the RSE's absence—will be informed of the Security Event. The RSE will act as the Incident Commander or the RSE will identify a person who will act as the regional Incident Commander (IC) for the incident.

5.2.2 The Incident Commander will perform a preliminary risk assessment, using the guidelines provided in *Appendix A - Initial Security Event Assessment*, to determine if a Security Incident has occurred and if further investigation is required.

5.2.3 If the Security Event is not determined to be an incident, the Incident Commander will record the event type (for statistical purposes).

5.2.4 If the Incident Commander determines an incident has occurred, the incident response process will be invoked. The RSE will assign an incident number which will be documented on Appendix *D Security Incident Report* form and tracked on the Security Incident Log.

5.2.5 The Regional Security Engineer, or designee, will notify the Emergency and System Security Breach contacts of the incident.

5.2.6 If the incident occurs at the ORCA Contractor, the Contractor will open a ticket and notify the RSE. The Contractor IC will run the incident, keeping the RSE continually updated on the status of the incident.

5.2.7 When the Contractor IC believes the incident is resolved, they will notify the RSE and the ORCA Operations Manager of root cause analysis, then request the incident be closed.

5.2.8 If the RSE accepts the ORCA Contractor resolution of the incident, the Contractor will document the incident and provide root cause analysis prior to requesting closure of the incident. The RSE will assign an incident number which will be documented on *Appendix D Security Incident Report* form and tracked on the Security Incident Log.

5.2.9 If the RSE does not accept the ORCA Contractor resolution, the investigation will continue until resolved with the incident approved for closure.

5.2.10 The Incident Commander will advise the Security Review Board and, if applicable, the Agency Security Representative (ASR) and Site Manager, if an incident requires further investigation, then continue assessing the incident and collecting further information and evidence.

5.2.11 The Incident Commander will perform containment, eradication and recovery activities until the incident is resolved.

5.2.12 If the incident comes from or is directly affects a specific agency, that agency's Site Manager and ASR will be informed of the incident. The ASR will be made Incident Commander and run the incident response, keeping the RSE continually updated on the status. Once the agency's Incident Commander believes the incident to be resolved, they will notify the RSE, who will determine if the incident can be closed. If the RSE accepts the agency resolution of the incident, the agency can close their incident process and begin documenting the incident.

5.2.13 If the Incident Commander determines that secure data has been affected during the course of an incident investigation, the Incident Commander will notify the Regional Program Administrator who will follow *Appendix E - Breach Response Public Communication and Notification*, and if applicable, invoke RCW 42.56.590 notification process.

5.2.14 Once the incident/breach has been closed, the Incident Commander will complete *Appendix D - Security Incident Report*, which will contain a root cause analysis, description of the incident activities, and lessons learned.

5.2.15 The RSE will maintain Reports on the Security Incident Tracking log.

6.0 POST INCIDENT ACTIVITY

Post incident activities are crucial in understanding the underlying factors that caused the incident and assist in preventing future incidents from occurring.

This process may include participants from outside of ORCA, with the relevant technical knowledge necessary to effectively review the incident as well as understand how to remediate technical or procedural issues.

All participating members must understand that this scenario is not to assess blame, but rather to discuss lessons learned from the incident with the goal of improving the overall security of the ORCA system.

All incidents are closed when sufficient information about the incident handling steps leading to resolution have been acquired and entered by Incident Commander (IC) into the ORCA record system. This includes recommendations about future mitigation actions to prevent re-occurrence of the incident.

6.1 Evidence Gathering and Handling

6.1.1 The IC shall maintain a detailed *Chain of Custody (Appendix C*) for all evidence, including but not limited to the following:

- Identifying information (e.g., the location, serial number, model number, hostname, media.
- Name, title, and phone number of each individual who collected or handled the evidence during the investigation.
- Time and date (including time zone) of each occurrence of evidence handling locations where the evidence was stored.

6.1.2 Many incidents cause a dynamic chain of events. From an evidentiary standpoint, a snapshot of the system as-is at the time of the incident provides excellent documentation and may prove more accurate than doing so after incident handlers, system administrators, and others have inadvertently altered the state of the system during the investigation.

6.1.3 The Regional Security Engineer (RSE) will inform the ORCA Operation Manager that a third-party forensic investigation is recommended or required. The ORCA Operations Manager will work through the Security Review Board to identify and approve the investigation contractor and its scope of work.

6.1.4 The ORCA Operations Manager will request root cause analysis from the applicable Agency or ORCA Contractor.

6.2 Prepare Report

6.2.1 The incident Commander will compile all information gathered during the course of the investigation into an incident report using the template provided in *Appendix D - Security Incident Report* for review with the Security Review Board.

6.2.2 This report will document the investigation process and shall:

- Contain all information discovered relative to the handling and response by the team.
- List investigation findings, including third party audit, when applicable.
- Document the process for determining inclusion in the notification group.
- Contain all information considered to determine the notification date and message.
- Include a copy of the official notification to affected individuals.

- Maintain a list of the names and other appropriate information of notified affected individuals.
- This list must remain confidential and kept in a secure location. Do not include the list with the report since the report may be subject to public disclosure requests.

6.3 Lessons Learned

A lessons learned meeting should be scheduled within several days or as soon as feasible following closure of the incident. Attendees should answer the following questions. Based on the nature of the incident, the following additional questions may arise:

- Exactly what happened and at what times.
- How well did staff and management perform in dealing with the incident.
- Did we follow the documented procedures.
- Are our procedures adequate. If not, what changes do we need to make.
- What information did we need sooner.
- Did we take any steps or actions that inhibited recovery.
- What would we do differently the next time a similar incident occurs.
- How can we improve information sharing with other organizations.
- What corrective actions can prevent similar incidents in the future.
- What additional tools or resources do we need to detect, analyze, and mitigate future incidents.

6.4 Prevent Future Incidents

6.4.1 From the information gathered at the lessons learned meeting, the Security Review Board will develop an appropriate prevention plan. The prevention plan will identify actions for the Agencies or ORCA Contractor aligned to the significance of the incident and whether it was a systemic compromise or an isolated instance and may include:

- Internal security audit of both physical and technical security, by agency or ORCA Contractor.
- Review of policies and procedures and any changes to reflect the lessons learned from the investigation.
- Review of employee training practices.

6.4.2 The resulting prevention plan may include a requirement for a compliance audit at the end of the process to ensure that the plan has been fully implemented. The Security Review Board shall determine if a compliance audit is required, and, if confirmed, determine scope and schedule of the compliance audit.

6.5 Tabletop Exercise

An annual tabletop exercise will be scheduled and include review of this Plan. Participants will include the Security Review Board, Site Managers, Agency Security Representatives and other agency or Contractor staff as applicable.

In the event of a Security Incident, the Plan will be exercised. Then, pending post incident review, the Security Review Board will confirm if the actual Security Incident may be considered sufficient evidence in lieu of a tabletop exercise.

7.0 AMENDMENTS

This Plan may be revised or amended following any incident, breach, or when new security processes/procedures are adopted by the agencies or the Joint Board.

The Appendices A-E may be revised by the ORCA Security Committee for review and approval by the ORCA Agencies.

Appendix A - Initial Security Event Assessment

Instructions for Submission

Incident Commander or designee will complete this assessment upon notification or observation of a Security Event.

Background	
Date and time the event was first reported	
How long has the event been occurring?	
How was the event found?	
Who found the event? What is the affiliation to ORCA?	
Who reported the event? If this is not the same person that found the event what is the relationship to the finder of the event?	
What has been done to this point?	
Are the systems currently functioning?	
Is the event information “credible” or from a reliable source?	
Name of Incident Coordinator (IC) for the agency or contractor. List phone number and work hours	
How many agencies are involved in the incident?	
Who else knows about the event both internally and externally?	
Scope	
Is there data involved?	
What type of data is involved in the incident?	
Where does the data reside?	
What category does the data fall into (credit card, PII, SSI, etc.)? Does this fall into RCW 42.56.590? Does the incident involve credit cards? Does the incident involve configuration data or SSI?	
Does the contractor have backups? When were they taken?	
What are the device types, operating systems, applications involved?	
Who administrates the devices involved?	
What type of exposure do these devices present?	
What customer impact would be noted if these systems are offline?	
Is there a danger of further damage? What are those indicators?	

Suspected Breach	
Are there indications of a suspected “Security Breach”?	
Is the suspected breach internal or external?	
Credit Card	
Are credit card numbers involved?	

Appendix B - Security Event Assessment

To be used when the Incident Commander is an Agency or Contractor (not the Regional Security Engineer)

Instructions for Submission

If you have a security event and suspect an incident or breach or receive information suggesting an incident or breach may have occurred, notify your Agency Security Representative as soon as possible but no later than 8 hours from the time initially detected.

Complete this form to collect initial incident details to assist in determining whether a breach has occurred and if so, the extent of the breach. This assessment will be used to complete the Security Incident Report (Appendix D).

***If the information comes from an external source, it is essential that that you not engage them in discussion suggesting that an incident or breach has occurred**. Provide the external source information to the Regional Security Engineer, who will initiate action in alignment with the ORCA Incident Response Plan.*

Contact Information	
Name:	Agency:
Date submitted:	Email:
Phone:	
Incident Information	
1. Date and Time of Incident	
2. Date and Time of Discovery	
3. Contact for person reporting incident or breach	
Name:	Agency:
Phone:	Email:
4. List additional employees and agency(ies) with knowledge of incident	
5. Detailed description of incident	
6. Describe any customer information involved	
7. Total number of customers potentially affected	
8. Additional pertinent information	

Appendix C – Chain of Custody

Instructions for Submission
Incident Commander, Incident Coordinator or designee with acquired evidence will complete one form per each piece of evidence as soon as an agency suspects an incident or breach occurred.

The custodian of the acquired evidence will track custody of the evidence. Each subsequent custodian will document chain of custody and maintain this original chain of custody form with the evidence.

Evidence
Identify Information (Serial number, hostname, IP address, MAC address, description, Log Data filename and media type)

Time / Date **Time zone** HH:MM DD/MM/YYYY PST	**Name of person who collected the evidence**	**Title / Phone number**	**Signature**	**Location of Secure Storage**

Appendix D - Security Incident Report - *Confidential*

Instructions for Submission
Incident Commander in coordination with Security Review Board will complete the Report. The Regional Security Engineer will assign the Incident Number and maintain the final Security Incident Report for the record.

Incident Details	
Incident Number:	IN-YYYYMMDD-HHMM Breach? Yes ☐ No ☐
Date/Time of Incident:	<Month followed by two-digit day, four-digit year – HH:MM EST/PST>
Location(s):	<Physical location of assets involved in the incident or alternatively of the reporting party>
Risk Severity:	<Choose from High, Medium or Low>
Incident Classification:	<Classify incident according to VERIS Framework> Ex.: External-Malware-Networks-Integrity (VERIS Threat Event # 169)
Reported by:	<Name and title of reporting party>
Additional Point(s) of Contact:	<List of names and titles of other principal incident stakeholders>

Incident Summary

<Outline the details of the incident, starting with the date and time when InfoSec learned of the incident and who reported the incident. Describe the most pertinent facts and details of the incident.>

EXAMPLE:

On January 27, 2019 at approximately 02:18 EST, Lead Council contacted Information Security (InfoSec) to report a security incident. Council had been contacted by the Federal Bureau of Investigation (FBI) who issued a report that a DNS server had been in communication with a rogue DNS server associated with criminal activity in the September 2018 timeframe. The FBI report indicates that one or more systems may have been infected with malicious software so as to surreptitiously participate in criminal online advertising and click fraud activity.

Incident Investigation & Mitigation

*<Outline the details of actions taken to investigate, assess and analyze the incident. Describe plans and/or actions taken to mitigate risks that are discovered over the course of the investigation. Be sure to include details of **who** took each action, **when** such action was taken, and **the outcome** of such action.>*

EXAMPLE:

The following actions were taken to investigate or mitigate risks associated with this Security Incident:

1. *InfoSec reviewed and analyzed the FBI report as well as further investigation details provided on the FBI's Victim Notification System (VNS).*

2. *InfoSec researched malicious domain and malware threats potentially associated with the rogue DNS IP address.*

a. *Historic domain lookups reveal that the last known domain associated with the IP address was "filesoffers.com" hosted by Genuine Network, Inc. out of Lincoln, NE. filesoffers.com was last registered to Sergei Nagornqj (nagornqj.sergei@gmail.com) of Krasnodar, Russia (phone # +1 798 392 4934, a non-functional U.S. telephone number).*

b. *Malicious code reports (Source: MalwareURL.com; VirusTotal.com) indicate that filesoffers.com was a malicious Web site hosting a Trojan horse downloader embedded within a PDF file. The URL it was being served out on the filesoffers.com site was: /get/file.php?q=Cauyog.pdf*

   The class lineage of this malicious code may allow remote attackers to completely control a victim system, send information to a remote attacker, and/or direct the victim's browser to a malicious Web site (Source: TrendMicro; TSPY_*, a family of Trojan spyware).

3. *Systems Engineering investigated the DNS server that resolved the malicious filesoffers.com domain. No signs of compromise were evident and the server was deemed healthy, but query logging was established to assist in future investigations. Since this logging has been enabled, there have been no signs of internal hosts attempting to resolve the filesoffers.com domain.*

4. *InfoSec investigated for any network audit trails to attempt to identify any internal systems that may have tried to resolve either the filesoffers.com domain or initiated outbound connections to the malicious DNS server. No network audit trails are in place to monitor, log or retain network connections for historical audit or investigation purposes. Therefore, further investigation into the internal infected source(s) was not possible.*

Findings and Recommendations

<During or at the conclusion of the incident, outline recommendations to better manage risks associated with the business process or computing systems involved in the incident. If relevant, include recommendations that are administrative (i.e., develop new policies or procedures, training, etc.) or technical (i.e., implement better logging, deploy an IDS, etc.) in nature.>

EXAMPLE:

The following is a summary of InfoSec's findings and recommendations applicable to this Security Incident:

1. *Asterisk servers located in remote offices are not configured to log call activity.*

   Recommendation: All asterisk servers should be configured to log all call activity. Logging allows for identification and review of patterns of suspect activity, such as attempts to bypass security mechanisms. Logging also enables more accurate assessment of the abuse, impact or damage to information assets after a Security Incident has occurred.

Additional Notes

Appendix E - Breach Response Public Communication and Notification

Appendix E provides steps to be taken by the Regional Program Administration Agency to prepare communication to stakeholders and issue public notice as required under RCW 19.255.010 and 42.56.590.

The Regional Program Administrator (RPA) will convene a meeting with the Incident Commander (IC), Regional Security Engineer (RSE), Chief Information Security Officer (CISO), and with the Regional Program Administration Agency's financial, legal and media relations representatives to assess impact of breach.

- The Incident Commander will provide assessment and impact of breach, including impact to the public, i.e., all cardholders, a subset if cardholders or if agencies have ability to collect fare. If suspension of fare collection is required, the Regional Program Administrator will request Board approval to direct the ORCA Contractor to.
- The Regional Program Administration Agency will:
  - Confirm if notification is required to law enforcement; assign notification to RSE or designee.
  - Confirm if notification is required from Fiscal Agent to card vendors.
  - Confirm if forensic investigation is required; work with Security Review Board to implement third party service.
  - Confirm message for public and other stakeholders (including the Joint Board, the Agencies and Contractor).
  - Confirm if news release is required; coordinate draft release through ST Public Information Officer, in coordination with regional PIOs.
  - Coordinate distribution of public messages through GovDelivery or current methodology.
  - Inform the Agencies and Contractor of outcomes.

The ORCA Agencies' merchant bank contacts and Visa, MasterCard notification protocols are maintained by the Fiscal Agent. In the event of a credit card breach, the Fiscal Agent will provide required notification to card vendors. Credit card companies will be notified whenever unauthorized disclosure of credit card information (e.g., unencrypted PANs) is suspected or confirmed. The relevant companies should be contacted via their prescribed methods.