Idaho Technology Authority (ITA)

ENTERPRISE GUIDELINES – G500 SECURITY PROCEDURES

Category: G585 – CYBERSECURITY INCIDENT AND BREACH RESPONSE REPORTING

CONTENTS

I. DEFINITIONS

See ITA Guideline G105 (ITA Glossary of Terms) for definitions

II. RATIONALE

This guideline assists agencies to establish incident response reporting procedures in alignment with Idaho State statute and ITA policies, standards, and guidelines pertaining to incident and breach response reporting.

III. INCIDENT AND BREACH RESPONSE ROLES AND CONTACT INFORMATION

NOTE: The following roles and contact information are for quick reference.

Entity	Role	Phone Number	Email Address
Information Technology Services CISO Office (ITS)	• Assists with incident response and management • Escalates incidents to Risk Management if a breach is determined • Oversees the ITS incident response governance program	Incident Response Line 208-605-4000	cyberrisk@its.idaho.gov
Office of Risk Management	• Provides breach management services to assist agencies	Risk Management Line 208-332-1869	

	• Provides access to State cyber insurance coverage • Provides professional breach management and legal support		
Office of the Attorney General (AG)	• Provides agencies legal advice in the event of a breach • Coordinates efforts with the Office of Risk Management	Contact your Agency Deputy Attorney General (DAG)	Contact your Agency Deputy Attorney General (DAG)

IV. GUIDELINE

Type	**State Entities**	**Timing Requirements**
Events	**Events** 1. Agencies have the discretion to escalate an event to the CISO Office in ITS for assistance and/or for community awareness. Such events may include, but are not limited to: a. Phishing attempts b. Abnormal network traffic c. Unsuccessful denial of service attempts, etc. 2. The CISO Office in ITS will distribute awareness communications to other state entities and partners such as DHS and/or MS-ISAC for their threat intelligence needs.	No specific time requirements. Preference is in a timely manner or as soon as possible for community awareness.
Incidents	**General Incidents** 1. Incidents may include, but are not limited to: a. Successful phishing attempts b. Violation of policy (e.g. technical or administrative) c. Took custody of an IT device for remediation efforts d. Reimaged system to remove malware, etc. e. Ransomware f. Denial of service	Within five (5) business days of discovery, agency will report incidents to ITS CISO Office. Initial report will be a best effort with information currently available, pending a full investigation. Weekly status

	2. Events that evolve into an incident will be investigated by the owning Agency and reported to ITS CISO Office via WebEOC *(see link in Section IV: Reference Documents)*. WebEOC must be completed to record the incident with ITS and to meet timing requirements for cyber insurance, should the incident evolve into a breach. 3. Investigation information must be provided about the incident (in the future, this will reference handling playbooks as a guidance.) 4. Agencies shall monitor the incident and provide periodic updates in WebEOC to ITS when new investigative information is available. a. NOTE: If needed, an agency is encouraged to contact the Incident Response line for assistance. 5. Agencies shall report the timely closure of an incident in WebEOC. **ITS Albert Sensor Notices** 1. Albert Alert is generated by the Albert Sensor (with an Albert ID number and a MS-ISAC SOC ticket number) and is assessed by MS-ISAC 2. MS-ISAC forwards the alert in the form of an e-mail to ITS Incident Response Coordinators (e.g. ITS CISO Office and Department of Homeland Security (DHS)). 3. ITS Incident Response Coordinators review the alert details and contacts MS-ISAC SOC to verify and check-in for additional details. 4. ITS CISO Office begin a log with date/time stamps of actions taken and communications. 5. ITS CISO Office immediately contacts the agency incident response coordinator from the ITS contact list (or the entity mentioned in the Albert notification). a. This contact is completed via phone or in person along with relaying the details of the attack and the recommendations in the Albert notification. b. **ATTN. AGENCIES: FOR SECURITY PURPOSES. DO NOT PASS THE CONTENTS OF THE ALBERT NOTIFICATION VIA GENERAL EMAIL.**	reports will be submitted to ITS. A full investigation report must be provided within 30-days. If a full investigation requires more than 30-days, contact ITS.

	6. State entity that causes the alert remediates incident (including following all MS-ISAC recommendations). This includes submitting an incident response form to ITS that contains both investigation and remediation information. a. ITS CISO Office reviews incident in WebEOC for the state entities remediation effort to confirm that all internal IP addresses identified in the Albert notification and any bad actor IP addresses are blocked from the Albert notification. **ITS MS-ISAC SOC TLP Yellow and Red Alerts** 1. TLP Yellow and Red alerts from MS-ISAC arrive in the form of an e-mail to the ITS incident response coordinator (e.g. ITS CISO Office and DHS). 2. The agency that causes the alert will read the details of alert and then contact MS-ISAC SOC to verify and get additional information. 3. ITS CISO Office will begin a log and time stamp actions taken and events that happened for the incident. 4. The ITS CISO Office will immediately contact the agency IT Security Coordinator that caused the alert from the ITS contact list or whoever the entity is mentioned in the notification. This will be performed via phone or in person who will relay the details of the attack and the recommendations in the notification. **a. ATTN. AGENCIES: DO NOT PASS THE CONTENTS OF THE YELLOW NOTIFICATION VIA EMAIL. If needed a hard copy of the yellow notification can be passed to the specific entity in question for remediation coordination and or communication via phone is allowed.** 5. The agency will remediate the incident in accordance with general incident handling procedures (see above) and any additional procedures the agency needs to perform including submitting an incident response form. 6. When the agency has remediated the alert, the agency needs to acknowledge that the entity in	

	question has blocked any bad actor IP addresses and that they have remediated any internal IP addresses identified in the yellow or red notification with the ITS CISO Office .	
Breaches	An agency's notification requirements for breaches are twofold. **1.** The agency has a responsibility to notify the Attorney General's Office (OAG), the Office of Risk Management (ORM), and the Office of Information Technology Services (ITS). a. NOTE: ITS customers will notify ITS via the ITS Service Desk which will notify the CISO of the breach. The CISO will immediately log the breach into Web-EOC which will electronically notify the ORM for coordination. This electronic notification to ORM does not alleviate the duty of the agency to directly notify the ORM of the breach. **2.** An agency has a responsibility to notify the Idaho residents that are affected by the breach or could potentially be affected by the breach. There are different requirements associated with each of these notifications, both of which are addressed below. <u>Agency responsibilities for notifying the **OAG, ORM, and ITS**</u>: Notifications to the OAG, ORM, and ITS shall not be later than 24 hours after discovery of a breach regardless of the determination of misuse. Notification to OAG, ORM and ITS are made by: 1. Contacting the Deputy Attorney General that advises the agency or calling the Attorney General's Office if the agency does not have an assigned Deputy Attorney General. 2. Completing the incident response form with investigation information that describes the breach, AND by alerting the ORM and ITS of the breach by calling: a. ORM at 208-332-1869, and b. ITS at 208-605-4000 If an agency does not have access to the incident response form, an agency can meet this notification	Within 24 hours of discovery to ITS CISO Office, Office of Risk Management (ORM), and the Attorney General's Office (OAG)

	requirement by sending the investigation information to: cyberrisk@its.idaho.gov AND by alerting the ORM and ITS of the breach by calling ORM at 208-332-1869, and ITS at 208-605-4000. Notification to the OAG and ORM is NOT required: When the breached data is in a form that is unusable, unreadable, or indecipherable to unauthorized individuals; meaning data that is either encrypted or destroyed in accordance with State policies and standards. In such instances the agency should not report a breach, however, the investigation information must still be reported as an incident (see ITA Policy P4510 – Cybersecurity Incident Reporting and ITA Guideline G510 – Cybersecurity Reporting Classification Template.) <u>Agency responsibilities for notifying affected Idaho residents:</u> 1. Notification to affected Idaho residents shall be made expediently and without unreasonable delay following the discovery of a cybersecurity breach if the agency believes that the information has or will be misused. Notification to affected Idaho residents must be consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach, to identify the individuals affected, and to restore the reasonable integrity of the computerized data system. 2. Notifications may be delayed when a law enforcement agency determines that notification would impede a criminal investigation. In such a case, notice must be made as soon as possible after a law enforcement agency advises the notification will no longer impede the investigation. 3. At the discretion of the agency, the agency can also utilize the counsel provided from ORM and/or the OAG in determining whether notification to affected Idaho residents should be delayed for purposes of investigation.	

	4. Refer to the “Notice” definition in § 28-51-104 for notice requirements. In considering notification responsibilities, the agency must also consider: 5. ITA Policies and Guidelines 6. The agency’s policies or the rules, regulations, or ITA polices and guidelines; The rules, regulations, procedures, or guidelines established by the agency’s primary or functional federal regulator. Notification to affected Idaho residents is NOT required: 7. When the cybersecurity breached data is in a form that is unusable, unreadable, or indecipherable to unauthorized individuals; meaning data that is either encrypted or destroyed in accordance with State policies and standards. 8. If, after an appropriate investigation or after consultation with relevant federal, state, and local agencies responsible for law enforcement, the agency determines that the misuse of the personal information has not occurred and is not reasonably likely to occur. 1.	

For ITS and ITS Customers

Type	ITS and ITS Customers	Timing Requirements
Events	1. ITS customer will contact the ITS Service Desk for support and direction on an event. Such events may include, but are not limited to: a. Phishing attempts b. Abnormal network traffic c. Unsuccessful denial of service attempts, etc. 2. ITS service desk will log event into Ivanti and route to ITS CISO Office for processing. 3. ITS CISO Office will review and determine if event should be escalated	See timing requirements above

Incidents	1. ITS customer will contact the ITS Customer Service Desk to report an incident. Incidents may include, but are not limited to: a. Successful phishing attempts b. Violation of policy (e.g. technical or administrative) c. Took custody of an IT device for remediation efforts d. Reimaged system to remove malware, etc. e. Ransomware f. Denial of service 2. ITS Customer Service desk will log incident into Ivanti with notifications sent to ITS Security Operations team and the ITS CISO Office 3. ITS Security Operations Team will provide incident handling and report findings to ITS CISO Office a. Investigation information must be provided about the incident 4. ITS CISO Office will receive report findings from ITS Security Operations Team and log into WebEOC 5. Both the ITS Security Operations Team and the ITS CISO Office will provide regular updates on need to know basis	See timing requirements above
Breaches	An agency's notification requirements for breaches are twofold: **1.** The agency has a responsibility to notify the Attorney General's Office (OAG), the Office of Risk Management (ORM), and the Office of Information Technology Services (ITS). **a.** NOTE: ITS customers will notify ITS via the ITS Service Desk which will notify the ITS CISO Office of the breach. The CISO will immediately log the breach into Web-EOC which will electronically notify the ORM for coordination. This electronic notification to ORM does not alleviate the duty of the agency to directly notify the ORM of the breach. **2.** The agency has a responsibility to notify the Idaho residents that are affected by the	See timing requirements above

	breach or could potentially be affected by the breach. There are different requirements associated with each of these notifications, both of which are addressed below. <u>Agency responsibilities for notifying the **OAG, ORM, and ITS**:</u> Notifications to the OAG, ORM, and ITS shall not be later than 24 hours after discovery of a breach regardless of the determination of misuse. Notification to OAG, ORM and ITS are made by: 1. Contacting the Deputy Attorney General that advises the agency or calling the Attorney General's Office if the agency does not have an assigned Deputy Attorney General. 2. Coordinating with the ITS CISO Office to verify incident was reported correctly in WebEOC. Contact information for ORM and ITS is: a. ORM at 208-332-1869, and b. ITS at 208-605-4000 Notification to the OAG and ORM is NOT required: When the breached data is in a form that is unusable, unreadable, or indecipherable to unauthorized individuals; meaning data that is either encrypted or destroyed in accordance with State policies and standards. In such instances the agency should follow incident procedures above. <u>Agency responsibilities for notifying affected Idaho residents:</u> 1. Notification to affected Idaho residents shall be made expediently and without unreasonable delay following the discovery of a cybersecurity breach if the agency believes that the information has or will be misused. Notification to affected Idaho residents must be consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach, to identify the individuals affected, and to restore the reasonable integrity of the computerized data system.	

	2. Notifications may be delayed when a law enforcement agency determines that notification would impede a criminal investigation. In such a case, notice must be made as soon as possible after a law enforcement agency advises the notification will no longer impede the investigation. 3. At the discretion of the agency, the agency can also utilize the counsel provided from ORM and/or the OAG in determining whether notification to affected Idaho residents should be delayed for purposes of investigation. 4. Refer to the “Notice” definition in § 28-51-104 for notice requirements. In considering notification responsibilities, the agency must also consider: 5. ITA Policies and Guidelines 6. The agency’s policies or the rules, regulations, or ITA polices and guidelines; The rules, regulations, procedures, or guidelines established by the agency’s primary or functional federal regulator. Notification to affected Idaho residents is NOT required: 7. When the cybersecurity breached data is in a form that is unusable, unreadable, or indecipherable to unauthorized individuals; meaning data that is either encrypted or destroyed in accordance with State policies and standards. 8. If, after an appropriate investigation or after consultation with relevant federal, state, and local agencies responsible for law enforcement, the agency determines that the misuse of the personal information has not occurred and is not reasonably likely to occur.	

IV. REFERENCE DOCUMENTS

- To access WebEOC go to: https://ioem.idaho.gov/webeoc/
- Idaho Code §§ 28-51-104, 28-51-105, 28-51-106, and 28-51-107; Definitions, Disclosure of Breach of Security of Computerized Personal Information by an Agency, Individual or Commercial Entity, Procedures Deemed in Compliance with Security Breach Requirements, and Violations respectively
- ITA Policy P4110 (Agency IT Security Coordinator)
- ITA Policy P4590 (Cybersecurity Incident and Breach Response Management and Reporting)
- ITA Standard S6010 (Cybersecurity Incident and Breach Response Management and Reporting)
- ITA Guideline G525 (Cybersecurity Incident and Breach Response Management)

V. CONTACT INFORMATION

For more information, contact the ITA Staff at (208) 605-4064.

VI. REVIEW CYCLE

Twelve (12) months

VII. REVISION HISTORY

02/18/2020 – Updated reporting contact information; added link to WebEOC.

06/18/2019 – Section III revised and updated.

Effective Date: May 30, 2019

CYBERSECURITY BREACH NOTIFICATION TEMPLATE
APPENDIX A

SAMPLE LETTER 1
Data Illegally Acquired: Credit Card (or Financial Account) Number Only

Dear _____,

We are writing because of a recent security incident at *[name of organization].*

[Describe what happened in general terms, what type of personal information was involved, and what you are doing in response.]

To protect yourself from the possibility of identifying theft, we recommend that you immediately contact *[credit care or financial account issuer]* at *[phone number]* and close your account. Tell them that your account may have been compromised. If you want to open a new account, ask *[name of account issuer]* to give you a PIN or password. This will help control access to the account.

To further protect yourself, we recommend that you place a fraud alert on your credit files. A fraud alert lets creditors know to contact you before opening new accounts. Just call any one of the three credit reporting agencies at a number below. This will let you automatically place fraud alerts with all of the agencies. You will then receive letters from all of them, with instructions on how to get a free copy of your credit report from each.

Experian	Equifax	TransUnion
888-397-3742	800-525-6285	800-680-7289

For more information on identify theft, we suggest that you visit the Federal Trade Commission at www.consumer.gov/idtheft. If there is anything *[name of organization]* can do to assist you, please call *[toll-free number].*

[Closing]

SAMPLE LETTER 2
Data Illegally Acquired: Driver's License (or Idaho ID Card) Number

Dear _____,

We are writing because of a recent security incident at *[name of organization]. [Describe what happened in general terms, what kind of personal information was involved, and what you are doing in response.]*

Since your Driver's License *[or Idaho Identification Card]* number was involved, we recommend that you immediately contact your local DMV office to report the theft. Ask them to put a fraud alert on your license.

To further protect yourself, we recommend that you place a fraud alert on your credit files. A fraud alert lets creditors know to contact you before opening new accounts. Just call any one of the three credit reporting agencies at a number below. This will let you automatically place fraud alerts with all of the agencies. You will then receive letters from all of them, with instructions on how to get a free copy of your credit report from each.

Experian	Equifax	TransUnion
888-397-3742	800-525-6285	800-680-7289

When you receive your credit reports, look them over carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for personal information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a report of identity theft. *[Or, if appropriate, give contact number for law enforcement agency investigating the incident for you.]* Get a copy of the policy report. You may need to give copies to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, we recommend that you check your credit reports every three months for the next year. Just call one of the numbers above to order your reports and keep the fraud alert in place.

For more information on identity theft, we suggest that you visit the Web site of the Federal Trade Commission at www.consumer.gov/idtheft. If there is anything *[name of your organization]* can do to assist you, please call *[toll-free phone number].*

[Closing]

SAMPLE LETTER 3
Data Illegally Acquired: Social Security Number

Dear _____,

We are writing because of a recent security incident at *[name of organization]. [Describe what happened in general terms, what kind of personal information was involved, and what you are doing in response.]*

To further protect yourself, we recommend that you place a fraud alert on your credit files. A fraud alert lets creditors know to contact you before opening new accounts. Just call any one of the three credit reporting agencies at a number below. This will let you automatically place fraud alerts with all of the agencies. You will then receive letters from all of them, with instructions on how to get a free copy of your credit report from each.

Experian	Equifax	TransUnion
888-397-3742	800-525-6285	800-680-7289

When you receive your credit reports, look them over carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for personal information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a report of identity theft. *[Or, if appropriate, give contact number for law enforcement agency investigating the incident for you.]* Get a copy of the policy report. You may need to give copies to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, we recommend that you check your credit reports every three months for the next year. Just call one of the numbers above to order your reports and keep the fraud alert in place.

For more information on identity theft, we suggest that you visit the Web site of the Federal Trade Commission at www.consumer.gov/idtheft. If there is anything *[name of your organization]* can do to assist you, please call *[toll-free phone number].*

[Closing]