Page 1 of 2 IR Playbook - Third Party Data Breach Notifications As of: 2/26/24

Information Security Incident Response Playbook
Third Party Data Exposure Notifications
Purpose. This playbook describes the steps to determine how to handle notifications regarding data exposures from
third party services that have a possible relationship with Stevenson accounts, mainly where Stevenson email accounts
were used to register for third party services.
Procedure
1. Triage.
a. Source of report.
i. The following are known, reputable sources:
1. Have I Been Pwned
2. Research and Education Networks Information Sharing and Analysis Center (REN-ISAC)
ii. Other sources will need to be evaluated by an OIT director for credibility.
b. Breach risk factors. The following areas should be considered in order to determine the appropriate risk
level:
Item High Medium Low
Time between
breach and
notification
Less than 6
months
6 months ʹ 2
years
More than 2 years
Number of
accounts
1000+ 11-999 1-10
Did third party
notify users?
Users were not
notified
Unconfirmed Users were
notified

Page 2 of 2 IR Playbook - Third Party Data Breach Notifications As of: 2/26/24

Correlation with
other sources
Confirmed
correlation from
other 3
rd
 party
Some correlation,
such as by the
owner
No other
correlation

2. Response actions.
a. An OIT director will review the individual factors to make an overall determination regarding the risk.
b. Follow the IR Playbook for Compromised Accounts for the response actions based on the risk rating.