IT Security Office - itso-g@vt.edu
Torgersen Tower, Ste 1300
620 Drillfield Dr.
Blacksburg, Virginia 24061

Handling Data Exposure Incidents

Contents

Responsibilities

Whenever Virginia Tech is notified of a potential data exposure, specific steps should take place in coordination with university officials to determine a course of action in compliance with federal and state regulations. The department responsible for the exposure should inform their department head of the incident and work with University Legal Counsel and the IT Security Office to determine appropriate action(s).

The department responsible for the exposure assumes primary responsibility for handling the exposure according to the procedure outlined herein. They should work with data stewards to verify the confidentiality of the data and take responsibility for developing a communications plan that includes any publicity, notification to individuals and others, and necessary remediation.

The group or department responsible for the data exposure is responsible for contacting individuals affected by the exposure and must consult with the IT Security Office and University Legal Counsel to develop a communications plan.

High-Risk Digital Data

High-risk digital data is defined by the Virginia Tech Standard for High Risk Digital Data Protection as data where protection is required by law or regulation and Virginia Tech is required to self-report to the government and/or provide notice to the individual if the data is inappropriately accessed. The standard defines six elements of Personally Identifiable Information (PII) as:

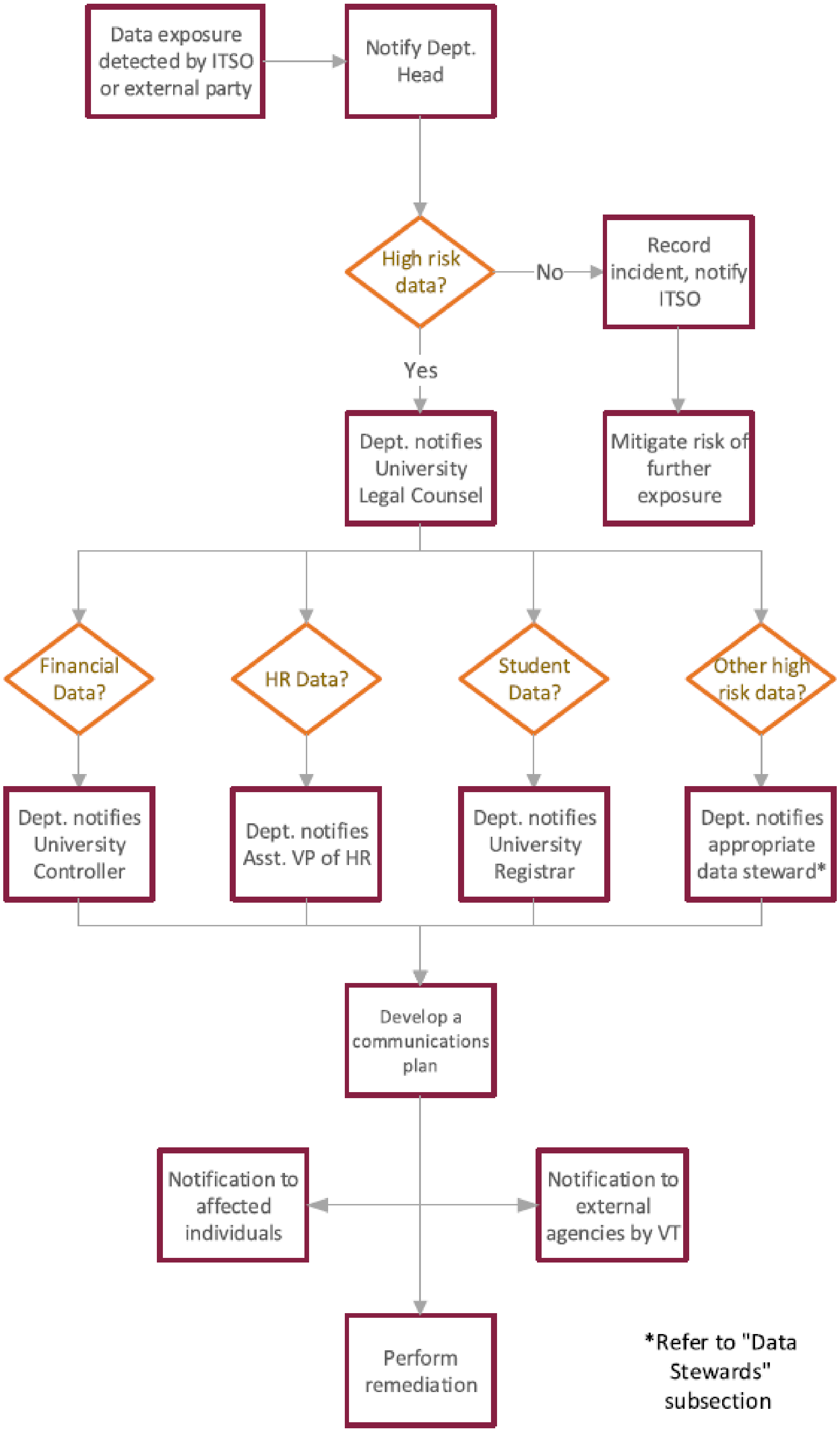
- Social Security Numbers (SSN)
- Debit card numbers
- Credit card numbers
- Financial account numbers
- Driver's license numbers (or any state-issued ID in lieu of driver's license)
- Passport numbers

Additionally, the standard defines protection requirements for the following data elements:

- Military ID numbers
- Medical & mental health history, treatment, or diagnoses information
- Health insurance policy numbers
- Student data (nondirectory information or items marked confidential) (FERPA)
- Export controlled research data (ITAR, EAR, CUI and others)

Please contact the IT Security Office with any questions regarding high-risk data. Additional information regarding data classification and examples can be found by reviewing the "Virginia Tech Risk Classifications" guidance: https://it.vt.edu/content/dam/it_vt_edu/policies/Virginia-Tech-Risk-Classifications.pdf

Data Exposure Response Procedure


Data exposure detected by ITSO or external party
Notify Dept. Head
High risk data?
No
Record incident, notify ITSO
Yes
Dept. notifies University Legal Counsel
Mitigate risk of further exposure
Financial Data?
HR Data?
Student Data?
Other high risk data?
Dept. notifies University Controller
Dept. notifies Asst. VP of HR
Dept. notifies University Registrar
Dept. notifies appropriate data steward*
Develop a communications plan
Notification to affected individuals
Notification to external agencies by VT
Perform remediation

*Refer to "Data Stewards" subsection

Notification Examples

Examples of contact letters have been provided below to help guide the process of contacting those who have had their data exposed. The examples utilize a scenario of data exposures through email and a stolen laptop. The contact template could easily be changed to reflect a data exposure through a lost or stolen digital storage device or any other scenario. Contact the IT Security Office and University Legal Counsel to coordinate a communications plan.

Example of High-risk Data Exposure via Email

<***DATE***>
<***Addressee***>
You are receiving this letter because on <***date***>, a handling error in our office resulted in a file containing some of your confidential data being sent to an incorrect e-mail address for which we cannot identify the owner.

The data file included the following information from your application to our program: <***List of data elements***>

We have no evidence that an unauthorized individual has actually utilized any of this information, and notice was sent to the recipient's address advising that the file was sent in error and requesting that it be destroyed. We are bringing this incident to your attention, in accordance with Virginia law, so that you can be alert to signs of any possible misuse of your personal identity.

As the situation develops, we will send additional messages regarding any further information which we are able to discover. Please monitor your email in the coming days for messages from our office. We have also changed our handling procedures such that files containing confidential data are transferred through methods other than e-mail. If you have any questions, please contact our department at <***department email***>.

We apologize for this lapse and for any inconvenience it may cause.

Sincerely,
<***Signature***>

Example of High-risk Data Exposure via Stolen/Lost Computer

<***Date***>

Dear <***student name***>:

Virginia Tech recognizes the importance of safeguarding your personal information. To that end, we have implemented strict administrative, technical, and physical safeguards to protect that information. However, even the most rigorous safeguards cannot guarantee protection against criminal conduct. Virginia Tech officials have been notified of the theft of a laptop computer which contained a file that held some of your personal information. Specifically, the file contained <***list of items***> from several years ago.

Although we believe this theft was directed at the hardware, and not its contents, we wanted to act preemptively to notify you of this situation and inform you of the risk. We do not have evidence that anything has been done with the information, but we are bringing this incident to your attention so that you can be alert to signs of any possible misuse of your personal identity. We will continue to monitor the situation, and recommend you take precautionary steps to guard yourself against any potential identity theft.

[We have established a website at <***(URL)***> to provide you with information]. If you determine that an account has been fraudulently established using your identity, you should contact law enforcement and the financial agency with which the account was established. The following references provide additional information about identity theft:

- FTC identify theft website at https://www.consumer.ftc.gov/features/feature-0014-identity-theft
- Social Security Administration Fraud Hotline at 1-800-269-0271
- Major Credit Bureau Numbers
    - Equifax 1-888-548-7878
    - Experian 1-888-397-3742
    - TransUnion 1-800-916-8800

As an additional safeguard, you may choose to place a temporary "fraud alert" on your credit report. Fraud alerts can help prevent an identity thief from opening any accounts in your name. You are encouraged to contact the toll-free fraud number of one of the three main consumer reporting companies to place a fraud alert on your credit report. Once you have placed a fraud alert with one of the bureaus, that bureau will send a request to the other two bureaus to do the same, so you do **not** have to contact all three.

Virginia Tech is committed to maintaining the privacy of present/past student information and takes many precautions for the security of personal information. Although social security numbers are no longer used for identification purposes in our automated systems, the files on the stolen laptop preceded the new identification policy and most records still contained the SSN. We sincerely regret any inconvenience this incident presents to you. If you have any questions, please contact our department at <***department email***>.

Sincerely,
<***Signature***>

Data Stewards

The Virginia Tech Standard for Administrative Data Management identifies university personnel who occupy the roles of data trustees and data stewards, so that members of the university community who may have a need to access data, make corrections, or better understand data definitions and data sensitivity will know to whom to direct their requests. The Division of Information Technology has established a website at https://it.vt.edu/resources/policies/adms.html which is intended to clarify who to contact for which types of data.

References

Standard for Administrative Data Management
https://it.vt.edu/content/dam/it_vt_edu/policies/AdministrativeDataManagementStandard.pdf

Virginia Tech Risk Classifications
https://it.vt.edu/content/dam/it_vt_edu/policies/Virginia-Tech-Risk-Classifications.pdf

Standard for High-Risk Digital Data Protection
https://it.vt.edu/content/dam/it_vt_edu/policies/Standard-for-High-Risk-Digital-Data-Protection.pdf

Revision History

Version 1.0 - Approved October 27, 2021, by Randolph Marchany, University Information Technology Security Officer

Version 1.1 - Updated data exposure response procedure graphic. Approved April 11, 2022, by Randolph Marchany, University Information Technology Security Officer