★ VIRGINIA ★
DEPARTMENT *of* ELECTIONS

Confidentiality/Privacy/FOIA

Part I: Security through Confidentiality
Part II: Transparency of Government Records
Part III: Security through Privacy

Arielle Anderson Schneider
Privacy Officer, Virginia Department of Elections

Part I: Security through Confidentiality

- Key concepts: CIA triad, scope of information, disclosure, and security mitigations
- What constitutes disclosure? And what should I do if I think I might have disclosed information to an unauthorized recipient?
- What types of information require special care?
- What are my responsibilities with regard to confidentiality and security?
- What type of information do I need to keep confidential?
    - Scope of information to which confidentiality and privacy expectations apply
    - Your agreement covers specifics about your internship location, regardless of content
    - Elections records and Security records have higher expectations of privacy and security

Core Principles of Security

Confidentiality

Integrity

Availability

Authenticity

- Which of the “original” 3 components of the triad will directly and constantly apply through every aspect of this internship?
  - Why did I add the last “A”

Core Principles of Security, continued

Presumption: All *information* regarding your work with locality security is privileged, confidential, and *cannot be disclosed* to unauthorized recipients. Some types of information are so sensitive that they cannot be transmitted electronically without additional security.

Information: All records and knowledge about entities (locality and ELECT), with higher care taken with election records and security records

Disclosure: (v) the act of making something known
(n) something (information) that is made known or revealed: something that is disclosed

Authorized Disclosure

1. locality authorizes you to share security information for legitimate business purposes with your teammates and the professor identified on your Internship Agreement.
2. you are authorized to share with the security team within ELECT (Johnathan, Amudha, Karen, Arielle) but not an ELECT liaison, for example
3. if you need to share with someone within the locality other than the GR, **ASK FIRST and DISCLOSE carefully**

Unauthorized Disclosure of Privileged Information

Disclosure includes

- Conversations with friends, unauthorized personnel
- Sending emails to the wrong recipient
- Sharing documents that were supposed to be redacted but were not

When/if you become aware of an unauthorized disclosure, notify Karen Hoyt-Stewart for further steps.

Internship Agreement

- The Intern shall maintain as confidential all information gained at the Internship Site. Violation of confidentiality may result in a referral for discipline at Virginia Tech and other lawful remedies. If the intern has questions about confidentiality, the intern needs to discuss the matter and take direction from the internship site supervisor prior to any dissemination of information.
- I am aware that any breach of this agreement, release of Confidential Information, or any abuse of my position, including, but not limited to, unauthorized access to records, disclosure of information from government or confidential records, alteration of records, and/or destruction of records or other similar acts, may result in disciplinary action through [University] Student Code of Conduct or otherwise, including possible termination of my position.

Confidentiality Responsibilities

Do not discuss topics, or share records that you are not authorized to disclose.

Considerations include:

- **Public domain.**
  - Is this information currently in the public domain? You still might not want to discuss it.
- **Permission.** Not forgiveness.
  - Anyone you know is currently authorized to provide you authorization.
  - Locality information → ask the local IT resource whether they can give permission or whether it should come from someone else
  - Election information → ask the GR
- **Perpetuity.** From this point on, includes interviews, presentations, Christmas cards, resumes, etc.

Security Responsibilities

Know the types of information and records that are particularly sensitive and take additional security actions to mitigate risks of unauthorized disclosure.

Sensitive information includes

- Personally identifiable information
- Elections records and information
- Security records and information

Additional security actions include

- Encrypting emails
- Password protecting documents
- Never using public wi-fi

Part II: Transparency

Public Access to Government Records

… and what that means for you

the Virginia Freedom of Information Act

Purpose of the FOIA as enacted by the Virginia General Assembly is to ensure the people of the Commonwealth:

- ready access to records in the custody of public officials
- free entry to meetings of public bodies wherein the business of the people is being conducted.

Because the affairs of government are not intended to be conducted in an atmosphere of secrecy, all public records and meetings shall be presumed open for inspection and copying upon request, unless an exemption is properly invoked.

- This statute also provides that the provisions of this Act “shall be liberally construed to promote increased awareness by all persons of governmental activities” and that any “exemption from public access to records or meetings shall be narrowly construed.”

the Virginia Freedom of Information Act: just to be clear

- All government records can be requested by the public, subject to exceptions
  - This includes any emails you send to locality or ELECT officials
  - A member of the public can request YOUR work product and communications
  - That work product would need to be carefully reviewed and redacted as needed

- Security records do not enjoy a blanket exception; they would need to be pulled, reviewed and redacted individually
  - Any reasonably segregable information in a responsive record must be released in response to a Freedom of Information Act (FOIA) request and non-exempt portions of a document must be disclosed unless they are inextricably intertwined with exempt portions. 5 U.S.C.A. § 552(b).
  - Even emails that are encrypted or marked as “confidential” will need to be reviewed and redacted individually

the Virginia Freedom of Information Act: EXCEPTIONS

- Under the Code of Virginia § 24.2-625.1. Voting equipment security, that records that describe protocols for maintaining the security of ballots on voting and counting equipment, or reveal the results of risk assessments of specific local electoral procedures, the release of which would compromise the security of any election, shall be confidential and excluded from inspection and copying under the Virginia Freedom of Information Act (§ 2.2-3700 et seq.).

the Virginia Freedom of Information Act: EXCEPTIONS

- Code of Virginia § 24.2-410.2. Security of the Virginia voter registration system, providing that "records describe protocols for maintaining the security of the Virginia voter registration system and the supporting technologies utilized to maintain and record registrant information, the release of which would compromise the security of the Virginia voter registration system, shall be confidential and excluded from inspection and copying under the Virginia Freedom of Information Act (§ 2.2-3700 et seq.)".

When a Records Release Goes Awry

- Why take all these precautions to mark documents and emails as exempt from FOIA?
  - PII release summer of 2017
  - Culture change
  - Knowledge sharing

- Recommendations for communications
  - SUBJECT LINE: CONFIDENTIAL – EXEMPT FROM DISTRIBUTION / FOIA per Va. Code § 24.2-625.1 & § 2.2-3705.2(14)
  - Watermark for classification level: CONFIDENTIAL or RESTRICTED

RECAP

- Keep all communications related to CNP professional in tone
- Clearly mark emails containing sensitive information
  - To protect the communication from outside eyes, ENCRYPT
  - To protect the communication from inside eyes, CLASSIFY and SUBJECT LINE.
- Just to say it again: Emails you send are likely to be reviewed by locality officials, therefore
  - mark your documents as DRAFT and CONFIDENTIAL or RESTRICTED,
  - encrypt your emails, and
  - note in the subject line (exempt from FOIA) as additional precaution

Part III:
Privacy through Security

Privacy and Security

- Complex passwords; use a password safe!
- Encrypt communications that contain sensitive conversations and/or sensitive data.
  - Team members amongst yourselves
  - Team to professor and vice versa
  - Team to ELECT and locality
- Basic Clean Desk:
  - Disable automatic logon functionality
  - Do not reuse passwords / do not share passwords
  - Always meet or exceed password complexity requirements
  - The computer you use must be yours alone

Privacy and Security

- Classify and password protect all workproduct so that it will be easily recognizable as qualifying for FOIA exemption
  - Complex Passwords essential
  - Data Classification: Put CONFIDENTIAL or RESTRICTED in the header of all your documents
  - Draft Status: Use a watermark to indicate your work is in DRAFT form.
    - Until a locality approves a document, the document will be DRAFT.
    - This is CRITICAL.

§ 24.2-410.2. Security of the Virginia voter registration system.

A. The State Board shall promulgate regulations and standards necessary to ensure the security and integrity of the Virginia voter registration system and the supporting technologies utilized by the counties and cities to maintain and record registrant information. The State Board shall, in consultation with representatives of local government information technology professionals and general registrars, update the security standards at least annually. Such review shall be completed by November 30 each year.

B. The electoral board of each county and city that utilizes supporting technologies to maintain and record registrant information shall develop and annually update written plans and procedures to ensure the security and integrity of those supporting technologies. All plans and procedures shall be in compliance with the security standards established by the State Board pursuant to subsection A. Each electoral board shall report annually by March 1 to the Department of Elections on its security plans and procedures. The general registrar and the Department of Elections shall provide assistance to the electoral board, upon request by the electoral board.

D. Records of the State Board or of a local electoral board, to the extent such records describe protocols for maintaining the security of the Virginia voter registration system and the supporting technologies utilized to maintain and record registrant information, the release of which would compromise the security of the Virginia voter registration system, shall be confidential and excluded from inspection and copying under the Virginia Freedom of Information Act (§ 2.2-3700 et seq.).

E. The State Board or a local electoral board may hold a closed meeting pursuant to the provisions of the Virginia Freedom of Information Act (§ 2.2-3700 et seq.) for the purpose of discussing protocols for maintaining the security of the Virginia voter registration system and the supporting technologies utilized to maintain and record registrant information, where discussion of such matters in open meeting would compromise the security of the Virginia voter registration system. Nothing in this subsection shall be construed to authorize a closed meeting to discuss any breach of security of the Virginia voter registration system.

F. Nothing in this section shall be construed to prohibit the release of information concerning any breach of security of the Virginia voter registration system.

case study: VRSS and CNP

VRSS-based Confidentiality Agreement

Scope

The Parties are exploring the security of the Virginia voter registration system, and collaborating on an annual review of locality security standards. In the course of these discussions, it will be necessary for each Party to disclose to each other confidential information regarding the existing security standards, assessments of local elections officials' security posture regarding the security and integrity of the Virginia voter registration system and supporting technologies used by counties and cities in the course of administering elections throughout the Commonwealth at both the state and local level.

Timeline

The Parties agree to be bound by the terms of this Confidentiality Agreement until and unless the VRSS material is made publicly available by the Virginia Department of Elections.

Public Access

The Parties agree that any requests by the public to receive copies of materials should be directed to the Department of Elections, which will be the entity responsible for responding to such requests for information.

Locality Election Security Confidentiality Requirements

To facilitate the exchange of information without compromising security or confidentiality, the Parties agree as follows:

- The Parties agree and acknowledge that records associated with the CNP program or your locality are privileged and may not be shared with persons who are not formally authorized.
- The Parties shall use reasonable efforts to maintain the confidentiality of CNP materials, whether disseminated through written, oral, or any other means.
- The Parties agree not to discuss the meetings or work of CNP with persons who are not members of the CNP community. If needed, a member may conduct discussions within localities' IT/Security departments; however, any discussions must be limited to hypothetical or theoretical exchanges with official local or state employees whose professional feedback may be helpful to the member or to the VRSS Advisory Group.

CIRCLING BACK TO THE BEGINNING

- Follow all the best practices you've learned over the course … security starts with you and your example might be the impetus for change
- Clearly mark and protect emails and workproduct containing sensitive information
  - To protect the communication from outside eyes, ENCRYPT
  - To protect the communication from inside eyes, CLASSIFY and SUBJECT LINE.
- ELECT has resources to assist – data classification charts, data retention, security templates
- If you have questions about any of this, contact Karen, your professors, or Arielle @ ELECT (Arielle.Schneider@elections.Virginia.gov)

Questions and Contact Info

Arielle Anderson Schneider
Arielle.Schneider@elections.Virginia.gov
(804) 801-6435