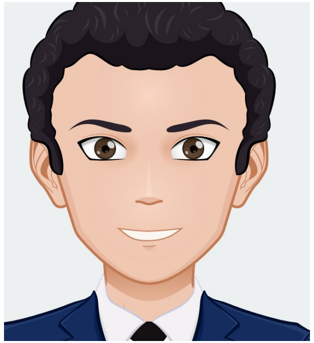
Policy Persona - Acceptable Use



Pablo is a general staff member of the staff who uses computing devices and network resources to conduct ORG business. He uses social media, and interacts with clients and co-workers daily. It is his job to help safeguard ORG data, equipment and culture..

Pablo uses a company issued computer, internet and other systems for all organization-related activities including email, files, internet and phone calls.

What does this impact?

Organization Data

Organization Systems

Organization Reputation and Integrity

Organization Culture

Practices good security with s**trong passwords, 2-factor verification** and necessary **updates**.

Conducts himself with **integrity and respect** for his co-workers and the ORG **mission**

Keeps **online activity** (email, social media and web sites) legal, **work-appropriate,** and uses respectful language

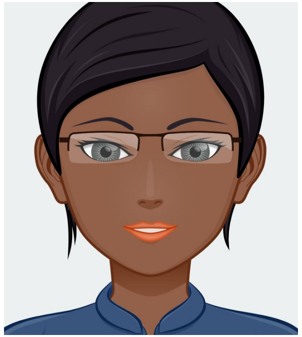
Respects intellectual property privacy, confidentiality and integrity of **data**.

Reports any data **security breaches, damage** or **loss** of equipment

Pablo uses **caution** in opening **unexpected links or attachments**, unless he has verified the sender's identity by another method.

Original Source: https://www.accessnow.org/cms/assets/uploads/2017/02/A-first-look-at-digital-security_DigiCopy.pdf

Policy Persona - BYOD



Irena uses her personal smartphone and tablet to access ORG systems, email, and files.

What needs protecting?

Passwords and accounts

Emails and files

Irena has her ORG email set up on her personal phone and also accesses other work related files and data.

To protect the data and device::

Irena uses a **password** on all devices

Irena **keeps an eye on her devices** and **eports a device loss or theft** immediately

Irena uses **caution when installing Apps t**o make sure they are **reputable**.

Irena is **aware** that ORG has the ability to **wipe** her device if necessary and keeps backups

Irena **does not store or download sensitive data** to her personal device(s).

Irena is **careful** when letting other people use her device to **close ORG accounts and files**

Original Source: https://www.accessnow.org/cms/assets/uploads/2017/02/A-first-look-at-digital-security_DigiCopy.pdf

Policy Persona - Organization-Issued devices

What needs protecting?

Carrie uses her ORG issued device only for work related items. She does not allow other users on her device and always keeps an eye on it. Though she may have to access sensitive data she uses the best practices to limit and protect it.

Carrie uses an ORG issued smartphone and laptop to access ORG systems, email, and files. As well as texts and phone calls.

Email and files

Files

Sensitive documents

To mitigate these vulnerabilities:

Carrie uses her **4G connection** when **secure WiFi** is not available.

Carrie **protect accounts** and the **device with strong passwords.**

Carrie **locks her devices** when not in use and does not allow other to use it

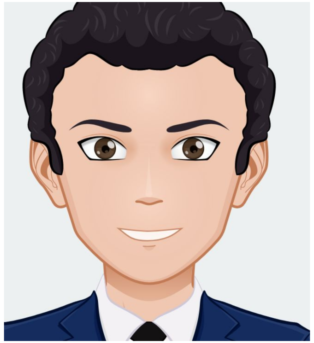
Carrie works to **understand clearly what types of communications are sensitive** and should be encrypted.

Irena **keeps an eye on her devices** and **reports a device loss or theft** immediately

Irena does not **install Apps** unless approved by IT

Original Source: https://www.accessnow.org/cms/assets/uploads/2017/02/A-first-look-at-digital-security_DigiCopy.pdf

Cybersecurity Persona - Staff



What needs protecting?

Paul is a general staff member of the staff who though he does not deal with sensitive documents still accesses organizational data and systems daily from office and home.

Paul uses his personal smartphone and computer for organization-related activities including email, Google Drive, texts and phone calls.

Sensitive information in emails and documents

Sensitive data on personal computing and mobile devices (BYOD)

Passwords and accounts

To mitigate these vulnerabilities:

All of his online accounts use **Two-Factor Authentication (2FA)**

Paul keeps track of account access with the **security checkups** offered by Google and other services.

All of his online accounts use **Two-Factor Authentication (2FA)**

Paul keeps computer OS, Antivirus and software **Up-to-date** on his personal devices.

Paul uses a **password manager** to ensure his passwords are complex, unique and he can notified if they are involved in breaches.

Paul uses **caution** in opening **unexpected links or attachments**, unless he has verified the sender's identity by another method.

Original Source: https://www.accessnow.org/cms/assets/uploads/2017/02/A-first-look-at-digital-security_DigiCopy.pdf

Policy Persona - Finance

Francine handles all the organizational finance and has access to bank accounts, credit card numbers, donations, wire transfers and items like petty cash and checks.

What needs protecting?

- Passwords and Accounts
- Email and communications
- Financial accounts
- Sensitive data on personal computing and mobile devices (BYOD)

Since Francine handles all the organizational finances and is often the recipient of phishing attempts it is important for her to have vigilance and awareness of socially engineered threats along with technical protections.

To mitigate these vulnerabilities:

Francine uses **2FA (two-factor authentication)** on all accounts for which it is available..

Francine uses a **password manager** to ensure her passwords are complex, unique and so she can notified if they are involved in breaches.

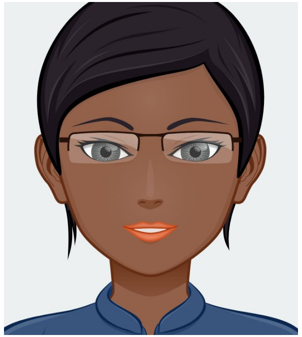
Francine **encrypts personal computing and mobile devices and protect them with strong passwords.**

Francine uses **caution** in opening unexpected links or attachments, unless she has **verified** the sender's identity by another method.

Francine keeps computer OS, Antivirus and software **Up-to-date** on his personal devices.

Francine **engages in security awareness training** and has a basic understanding of how social engineering can be used to breach security

Original Source: https://www.accessnow.org/cms/assets/uploads/2017/02/A-first-look-at-digital-security_DigiCopy.pdf



Policy Persona - C Suite

As the ED Erin has her hand in all aspects of the organization. She has access to sensitive data, finances, HR and social media.
She handles strategies, interdepartmental communications and donor outreach.

What needs protecting?

Passwords and accounts

Sensitive information in documents and emails

Sensitive data on personal computing and mobile devices (BYOD)

Policy culture

As the ED Erin is responsible for ensuring that Policy is appropriately prioritized within her organization and models desired Policy behavior for staff.

To mitigate these vulnerabilities:

Erin uses a **Virtual Private Network (VPN)** to access the internet anytime she is on an unknown or insecure network.

Erin **encrypts personal computing and mobile devices and protects them with strong passwords.**

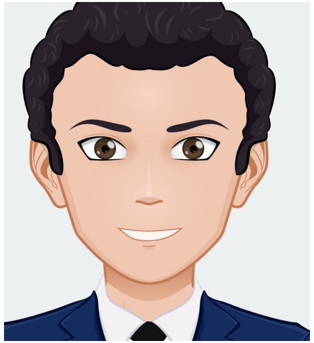
Erin uses **2FA (two-factor authentication)** on all online accounts for which it is available..

Erin takes time to understand Policy risks to her organization and **prioritizes security efforts** appropriate to mission

Erin uses **caution** in opening unexpected links or attachments, unless he has **verified** the sender's identity by another method.

Erin nurtures a **security culture** by responding thoughtfully to reported risks or errors from staff.

Original Source: https://www.accessnow.org/cms/assets/uploads/2017/02/A-first-look-at-digital-security_DigiCopy.pdf



Cybersecurity Persona - IT

Idris is responsible for all of the organizational data and systems. He has Administrative rights to all systems and access to all files.

What needs protecting?

- Passwords and accounts
- Hard Drive and data files
- Computing habits and practices
- Sensitive data on personal computing and mobile devices (BYOD)

Idris access many administrative accounts on a daily basis and has full access to all of the organizational data. His accounts, habits and computing devices need special attention to security. He also needs to be current on new threats to better inform staff and protect the organization.

To mitigate these vulnerabilities:

Idris uses **2FA (two-factor authentication)** on all accounts for which it is available..

Idris nurtures a **security culture** by responding thoughtfully to reported risks or errors from staff.

Idris uses a **password manager** and **strong, 30-character+ passwords** with special characters and numbers and is notified if they are involved in breaches.

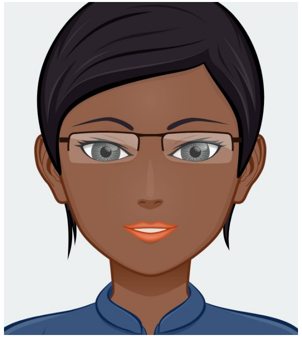
Idris uses a **super user** account to access administrative rights and not his regular user account.

Idris uses a **Virtual Private Network (VPN)** to access the internet anytime she is on an unknown or insecure network.

Idris regularly **attends security training** and keeps up-to-date on new threats and updates staff and management.

Original Source: https://www.accessnow.org/cms/assets/uploads/2017/02/A-first-look-at-digital-security_DigiCopy.pdf

Cybersecurity Persona - Protected Data



Carrie works with sensitive data including items subject to PHI/PII and HIPPA compliance. In order to protect her clients, her organization and herself, Carrie is reviewing all of her communications and data storage practices for security and privacy. communications are sometimes sensitive and need to be protected to ensure the confidentiality of collaborators

What needs protecting?

- Protected information
- Digital Communications
- Sensitive documents
- Sensitive data on personal computing and mobile devices (BYOD)

Carrie spends her workdays reviewing case files, interviewing people and communicating with clients and colleagues via text, email and phone. The vast majority of this information must be kept confidential or Jane's clients could be at risk as well the integrity of her organization.

To mitigate these vulnerabilities:

Carrie uses a **Virtual Private Network (VPN)** to access the internet anytime she is on an unknown or insecure network.

Carrie **encrypts personal computing and mobile devices and protect them with strong passwords.**

Carrie uses **2FA (two-factor authentication)** on all online accounts for which it is available..

Carrie works to **understand clearly what types of communications are sensitive** and should be encrypted.

Carrie uses a **password manager** to ensure her passwords are complex, unique and so she can notified if they are involved in breaches.

Carrie engages in **security and compliance training** and has a strong understanding of how social engineering can be used to breach security.

Original Source: https://www.accessnow.org/cms/assets/uploads/2017/02/A-first-look-at-digital-security_DigiCopy.pdf

Policy Persona Template (Sample)

Ricky is an activist and blogger who calls attention to humanitarian issues around the world. Ricky's work is constantly under scrutiny by various organizations and his online accounts are regularly watched and susceptible to hacking and interception.

Due to rising safety concerns, Ricky is considering **encryption of all data and communications** with his team.

What needs protecting?

- Hard drives, data files, research papers
- Social media accounts
- Correspondence with other activists
- Government Sources

Over many years of hard work, Ricky has a substantial amount of content on his blog. He has many files full of research, plans and data that must be kept confidential - Integrity is everything in his line of work. Ricky is concerned that his information may be intercepted by foreign agencies who are not sympathetic to his cause.

To mitigate these vulnerabilities:

- Ricky uses a **Virtual Private Network (VPN)** to access the internet securely when connecting to wi-fi in public places.
- Ricky **encrypts** all of his email communications.
- All of his online accounts use **Two-Factor Authentication (2FA)**
- Ricky **encrypts all sensitive files, hard drives and external media.**
- Ricky creates **strong, 30-character+ passwords** with special characters and numbers organized by a **password manager.**
- Ricky **regularly clears out his chat history** to prevent previous communications falling into the wrong hands.

Original Source: https://www.accessnow.org/cms/assets/uploads/2017/02/A-first-look-at-digital-security_DigiCopy.pdf