We do this by delivering tech services, education, and training that help nonprofits and communities thrive.

NONPROFIT TECH SERVICES:

- Managed IT Support
- Cloud Services
- Strategic Consulting
- Security & Compliance
- Data Support
- Machine Learning & AI
- Community Integrated Design

NONPROFIT EDUCATION & TRAINING:

- Reports
- Consumer Guides
- Assessments
- Workbooks & Articles
- Online Training
- Free Webinars

WORKFORCE DEVELOPMENT:

ITWorks & CXWorks: Free IT and Customer Experience training programs

PunchCode:
12-week immersive programming bootcamp

TECHIMPACT®

WHY TECH IMPACT?

We've helped thousands of organizations use technology to make a bigger and better impact on the communities they serve.

WE GET IT.

We're a nonprofit too.

WE TRULY CARE.

Our first priority is to help.

WE'RE AGILE.

We constantly evolve to address changing landscapes.

WE DELIVER.

We work with the brightest minds in tech to bring you superior products and services that are affordable.

WE COLLABORATE.

We work with tech and corporate powerhouses to provide you with the best tools and platforms.

KAREN GRAHAM

Managing Director of Education & Outreach, Tech Impact

Pronouns: She/Her
karen@techimpact.org

Karen is a sought-after speaker, trainer, writer, and consultant with expertise in technology leadership and innovation, nonprofit software, and digital strategy. As Tech Impact's Director of Education and Outreach, she leads the Idealware team of researchers, presenters, and writers who create technology information resources designed to help nonprofit leaders put their vision into action.

DAN GETMAN

Senior Manager of Donor Relations

Pronouns: he/him
dgetman@mannapa.org

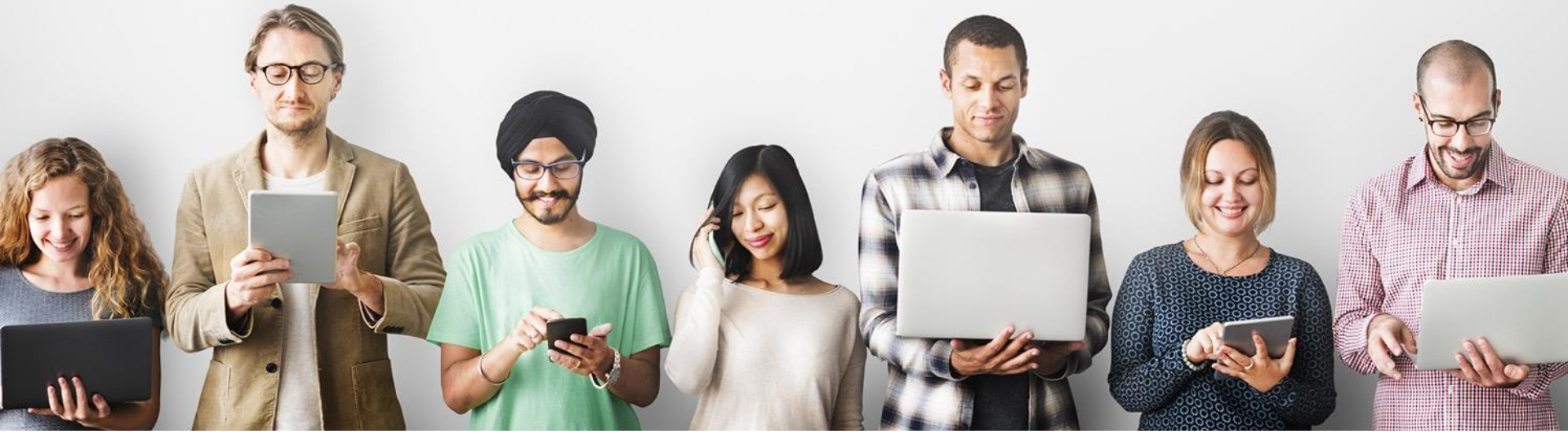
Dan oversees the individual fundraising at MANNA, a Philadelphia-based nonprofit that supplies medically appropriate meals to individuals facing serious illness. Having witnessed the fundraising landscape evolve over the last decade, he truly enjoys finding new ways to incorporate technology into the nonprofit sector. He currently is also responsible for MANNA's CRM database, website maintenance, and tech security.

LEARNING GOALS

1. Understand what should be in your Acceptable Use and IT Security policies.
2. Weigh pros and cons of different approaches to Bring Your Own Device.
3. Get better at gaining staff support and compliance.

LET'S CHAT

What is your organization's biggest hurdle in establishing tech policies today?



TECHIMPACT®

WHY EVEN HAVE POLICIES?

- Liability
- Discipline
- Actual behavior

GOOD PEOPLE, BAD CHOICES

Average cost of a data breach: $3.92M

55% of organizations reported that staffers caused a data breach or security incident

2016 *Cost of a Data Breach Report* – Ponemon Institute, 2019 *Cost of a Data Breach Report* – Ponemon Institute

WE ALL NEED GUIDANCE

Good policies help good people understand what's safe and what isn't.

WHAT SHOULD BE IN YOUR POLICY?

BASIC POLICY RECIPE

- State the purpose
- Explain the risks
- Specify the scope
- Describe the consequences
- Note exceptions

ACCEPTABLE USE

A guide to the overall use of your networks and equipment.

SECURITY

How to protect your data.

BRING YOUR OWN DEVICE

Considerations for employees using personal devices in the workspace.

INCIDENT RESPONSE & DISASTER RECOVERY

What to consider in case things go wrong.

REMOTE WORK

Considerations for employees who work outside of the office.

SOCIAL MEDIA & DIGITAL COMMUNICATION

Guidelines for how to represent the organization.

ACCEPTABLE USE

UPKEEP

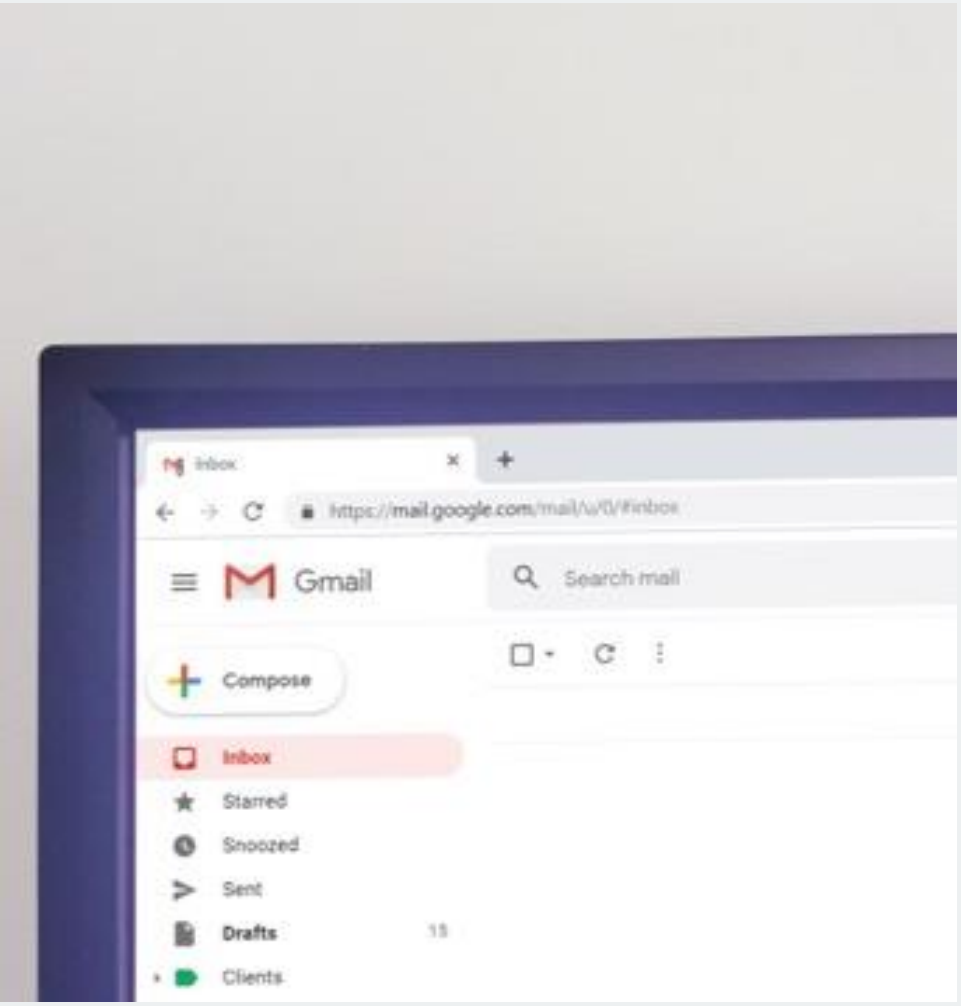
Are there times when a user is responsible for upkeep of equipment?

SOFTWARE INSTALLATION

Who gets to install applications, and which ones?

What about update protocols?

EMAIL USE



- Will you limit person use of email?
- Do your team members know not to spam?
- Are there guidelines for attachments?
- Will you monitor email?

MORE ACCEPTABLE USE TOPICS

Which of these are covered under your policies?

- ❑ Malicious Software
- ❑ Unintentional Malware
- ❑ Personal Commercial Use
- ❑ Playing Games
- ❑ Pornography
- ❑ Knowingly Causing a Breach
- ❑ Network Disruption
- ❑ Intercepting Data
- ❑ Getting around security
- ❑ Interfering with Operations
- ❑ Sharing Personal Information


SECURITY

WHEN IS IT OK TO SHARE DATA?

Do you have partnerships or other data-sharing arrangements?

Where is that data stored and how is it shared?

WHO HAS ACCESS TO WHAT DATA?

Does everyone have access to all data at all times?

If not, specify who should be able to see particular types of data.

WHAT MUST BE BACKED UP?

Establish guidelines for where and how to store files.

TECHIMPACT®

PASSWORD POLICIES

What needs a password?

How often should they change?

Set standards (e.g. number and type of characters).

OTHER REQUIREMENTS?

- No sharing.
- No patterns or easily identifiable information (e.g., office address).
- No reusing passwords.
- No writing passwords down.
- No emailing passwords.

PASSWORD MANAGERS

Many of your rules can be built into password management software. If you choose a password manager, you'll want to require staff members to use it.

DEVICE LOCKS

Your password and screen lock policies should also apply to personal devices used for work.

INCIDENT RESPONSE

What if you fall victim to cyber crime, data loss, or electrical or internet outages?

TECHIMPACT®


BRING YOUR
OWN DEVICE

POLL

Do staff members at your organization do work on their personal devices (phones, tablets, laptops, etc.)?

STAFF MEMBERS BENEFIT

It’s easier to manage a flexible schedule and do work “on the go.”

Personal devices are more familiar.

WHAT COULD GO WRONG?

- Mobile devices get lost or stolen.
- Work is done on insecure networks.
- Staff members are not downloading the latest patches and security software.
- People might leave—and take data and credentials with them.

WHO IS ALLOWED TO USE PERSONAL DEVICES?

You might want to keep the group small so that the situation is easier to control.

WHAT DEVICES ARE THEY ALLOWED TO USE?

Make as thorough a list as possible.

ARE SPECIFIC ACTIVITIES RESTRICTED?

For example, maybe you allow email access on a phone, but prohibit users from accessing your organization's CRM system via a mobile device.

WHAT APPS ARE OK?

Some organizations keep a strict “white list.” Others leave it to staff discretion.

DEVICE ENCRYPTION

You should require that the device has encryption and that it's turned on.

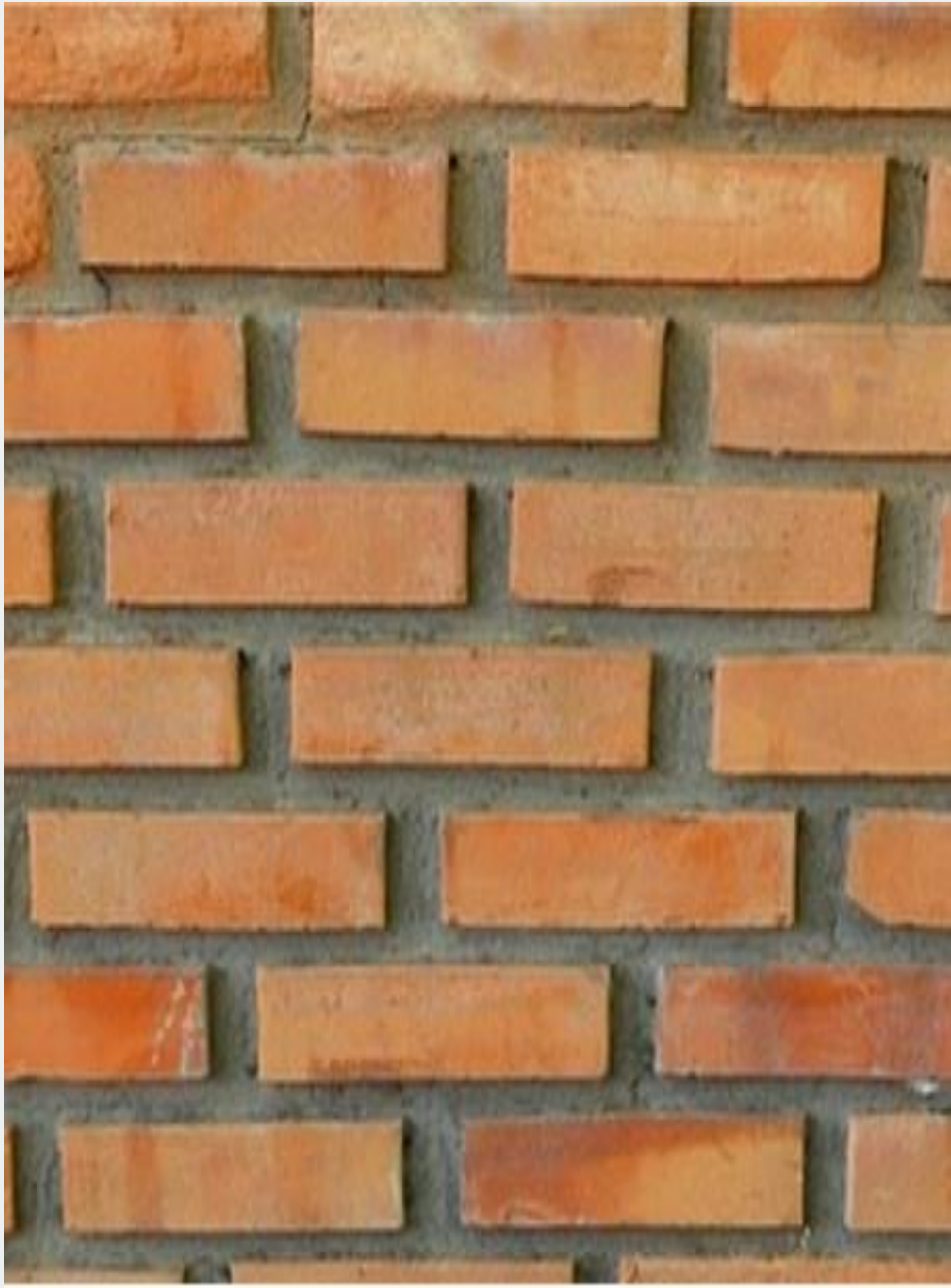
GUIDANCE ON NETWORKS

Many public Wi-Fi networks are insecure.

WI-FI

A few suggested requirements:

- Firewalls installed and updated
- Password protection
- Encryption



MOBILE DEVICE MANAGEMENT

Software exists to help you make sure updates are run and to control access to data if the staff member leaves.

ACTIVITY

Let's chat. Type your answer in Questions:

Do you have a restrictive BYOD policy or a supportive one? What do you like or dislike about this?

DEVELOPING AND USING POLICIES

SOLICIT INPUT

Other perspectives can help you see potential issues or loopholes you've overlooked.

MAKE THEM ACCESSIBLE

Keep your policies in a place where anyone can find them.

REVIEW PERIODICALLY

Are these still the right policies? Has technology or the way your organization works changed recently?

START CONVERSATIONS

Bring out your policies periodically during staff meetings or training sessions.

EXAMPLE: ANIMAL RESCUE LEAGUE OF BOSTON

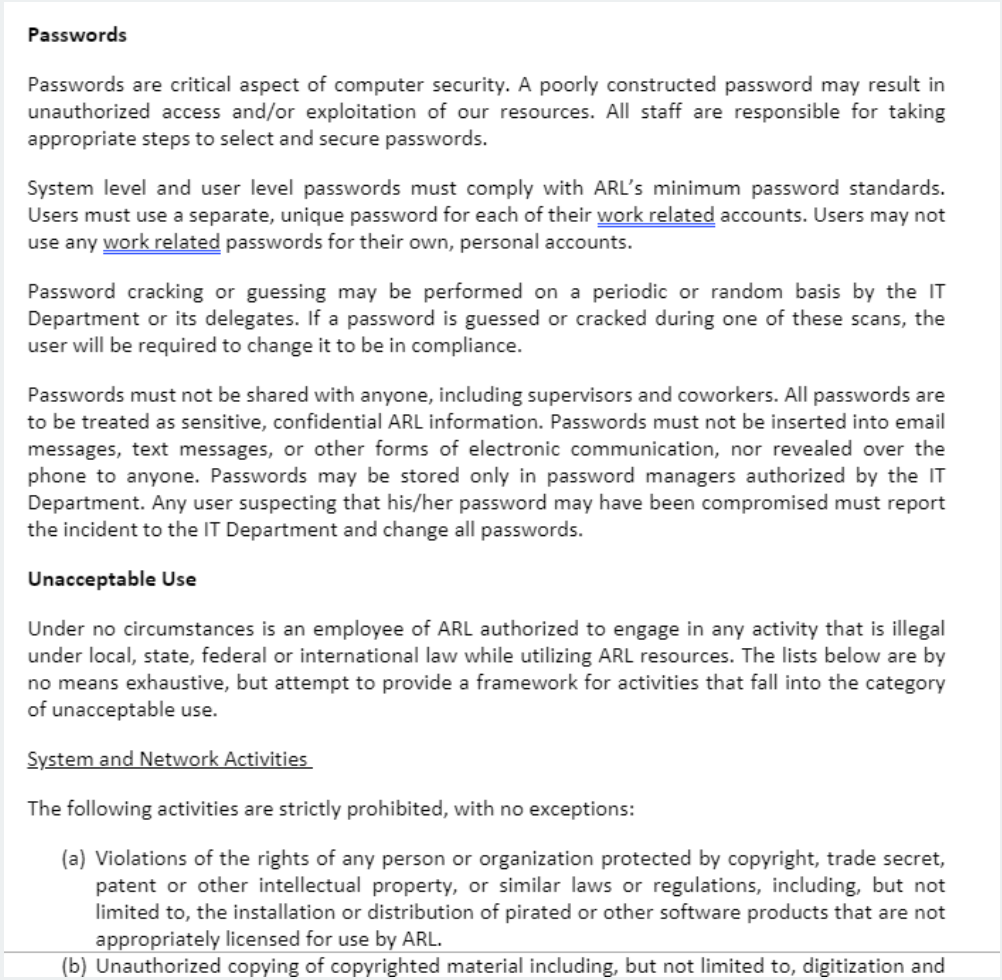
ARL is A 120-year-old organization with three locations and 120 staff.

Protecting data was important to them.

REVISING POLICES

They re-wrote acceptable use and password policies to follow an international standard.

The board approved the policies. They are part of the employee handbook.



Passwords

Passwords are critical aspect of computer security. A poorly constructed password may result in unauthorized access and/or exploitation of our resources. All staff are responsible for taking appropriate steps to select and secure passwords.

System level and user level passwords must comply with ARL's minimum password standards. Users must use a separate, unique password for each of their work related accounts. Users may not use any work related passwords for their own, personal accounts.

Password cracking or guessing may be performed on a periodic or random basis by the IT Department or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance.

Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive, confidential ARL information. Passwords must not be inserted into email messages, text messages, or other forms of electronic communication, nor revealed over the phone to anyone. Passwords may be stored only in password managers authorized by the IT Department. Any user suspecting that his/her password may have been compromised must report the incident to the IT Department and change all passwords.

Unacceptable Use

Under no circumstances is an employee of ARL authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing ARL resources. The lists below are by no means exhaustive, but attempt to provide a framework for activities that fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

(a) Violations of the rights of any person or organization protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of pirated or other software products that are not appropriately licensed for use by ARL.

(b) Unauthorized copying of copyrighted material including, but not limited to, digitization and

BALANCING CONVENIENCE AND SECURITY

People weren't thrilled about long, complex passwords.

The compromise: 10 characters. They also removed the requirement to update every 90 days.

They did all-staff training and a quiz on password practices.

Actual slide from their staff training

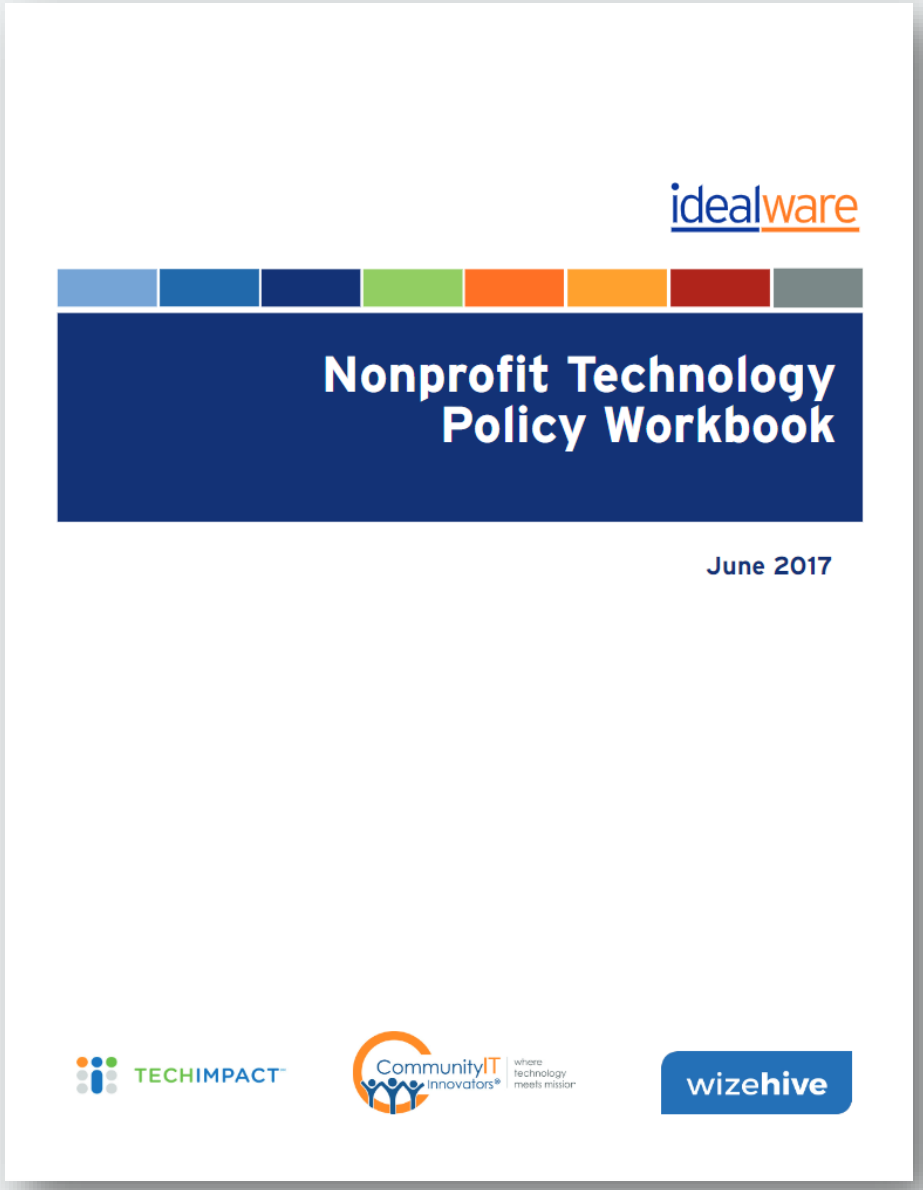
“Don’t discount how much is process versus substance. You need user input in order to create something that works for the culture and organization.”

~Constance de Brun, ARLB

NONPROFIT TECHNOLOGY POLICY WORKBOOK

A free guide to create and document policies for the acceptable use of technology and networks, personal devices for work, how to provide IT guidance to “accidental techies,” how to respond to an IT incident, and how to recover your technology after a major disaster.

https://offers.techimpact.org/reports/nptechpolicyworkbook/



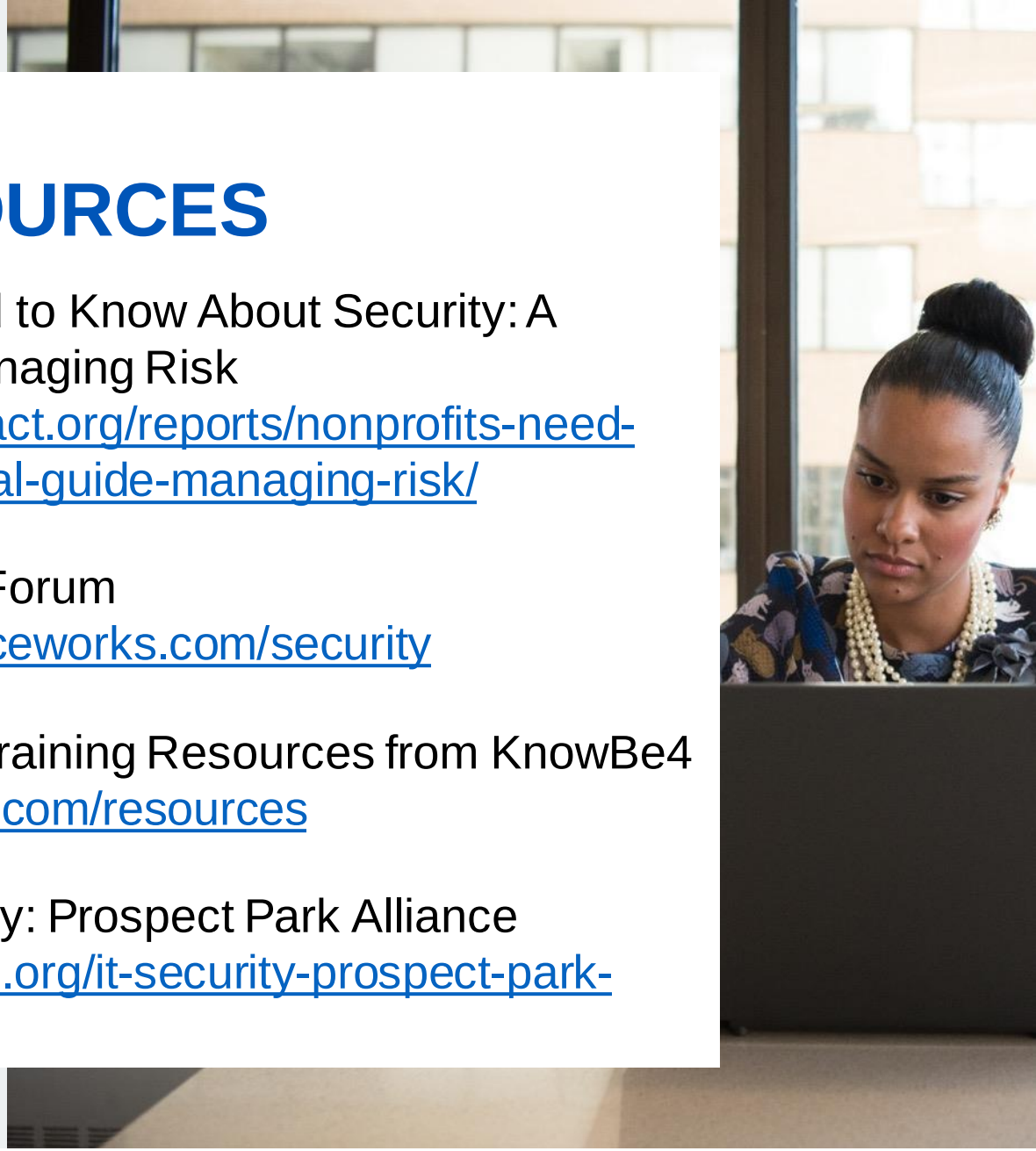
MORE RESOURCES

What Nonprofits Need to Know About Security: A Practical Guide to Managing Risk
https://offers.techimpact.org/reports/nonprofits-need-know-security-practical-guide-managing-risk/

Spiceworks Security Forum
https://community.spiceworks.com/security

Security Awareness Training Resources from KnowBe4
https://www.knowbe4.com/resources

IT Security Case Study: Prospect Park Alliance
https://www.idealware.org/it-security-prospect-park-alliance/



QUESTIONS?

Next Course

Remote Program Delivery

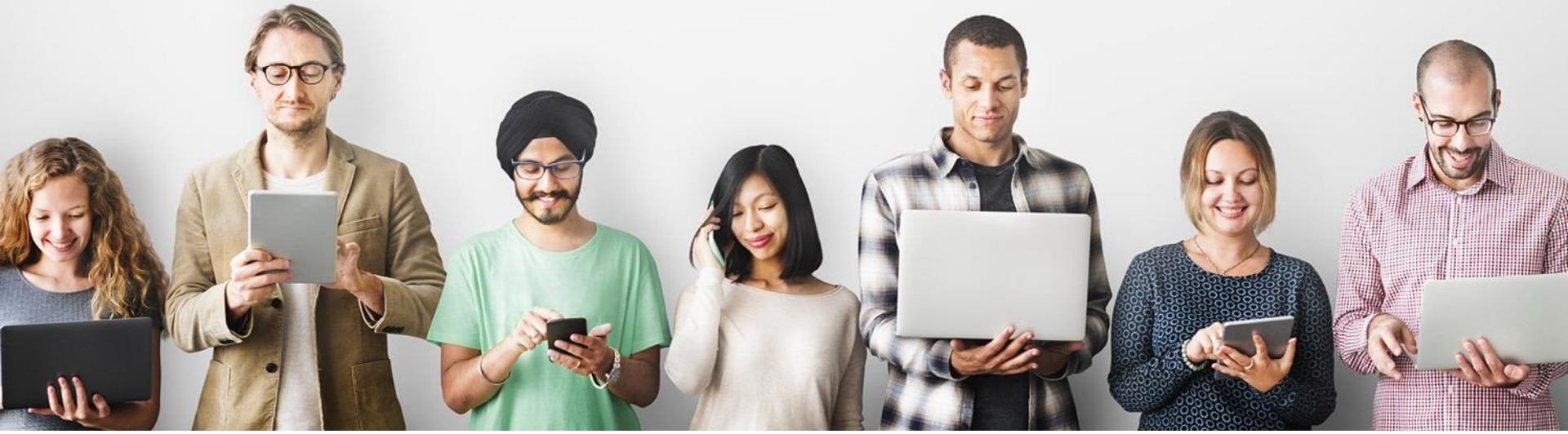
September 22, 23, 24, 1-2:30 PM EST

TECHIMPACT®

ACKNOWLEDGEMENTS

Thanks to the following who contributed to the development of this curriculum:

Constance de Brun, Dan Getman, Karen Graham



TECHIMPACT®

THANK YOU

Karen Graham: karen@techimpact.org

Dan Getman: dgetman@mannapa.org