Creating organisational security policies

What makes a good policy?

- keep it short and concrete
- focuses on goals, roles, responsibilities and tasks
- covers relevant security aspects (personal, office, travel, devices, etc.)
- clearly differentiates between what needs to be done once, regularly or all the time
- helps the reader to take action (spells out internal support, links to resources)
- clear link to organizational mission and identity
- is part of the main working space of an organisation, reflects its (visual) identity
- includes protective measures and incident response

What makes a bad policy?

- focused only on documentation of tools
- one that cannot be found by staff
- can only be understood by experts, champion or IT staff
- too aspirational and too far away from actual practices
- quick hack of a template, bad recycling of other policies
- is one giant document that does not differentiate between different needs and responsibilities

Goals

- Clear standard of practice within the organization.
- Ensure sustainability of practice
- Creating organizational consensus
- Establish initially and use dynamically as organization incorporates practices/environment or organization changes

Prerequisites

- Existing workflow and program activities
- Initial assessment, including resources
- Priorities
- Organigram
- Helpful: existing templates

Elements to be included

- Buy-in and strategy to implement, enforce, and inform policy
- Communication policy
    - social media
    - Email
    - Chat
    - Mobile
    - Branding practices and signatures
    - PGP usage, key storage, publishing keys, subject lines
- All should cover access control measures, levels of encryption, personal vs work usage
- Data managements policy
    - Where is stored? (cloud, local, etc)
    - Access control (new hires, employees leaving, different levels of access)
    - Data retention
    - Data deletion
    - Backup
    - Encryption
    - Password management
    - File naming and storage structure
- Equipment policy
    - Personal use
    - Taking home
    - Installing software

In this page:

Additional resources:

Baseline Organisational Policies and Practices

by Michael Carbone
This is a draft of a resource that came out of envisioning the next iteration of the Responsible Data Forum's Organizational Security Atomized Plan, and reframing it as a guide towards implementation within a group. In this reframing I have relied heavily on the content of the Organizational Security Atomized Plan itself, Internews' SAFETAG organizational assessment framework, and other resources listed in the resources section.
https://github.com/mfc/baseline-org-policies

Security Checklists

by iecology
The documents in this repository comprise a set of digital security checklists for use by US based non-profit organizations with a focus on human practice and organizational management. One checklist is oriented towards assessing an organization's readiness to take on this type of work. Additional documents represent framing information and a glossary.
https://github.com/iecology/security-checklists

    - Pirated software
    - Anti-Virus
    - Updates
    - Disposal of devices
- Training
    - When does training happen?
    - How often?
    - Self-learning resources?
    - Funds for professional development
- Employee leaving
    - What to exptect when you leave the organization
    - Email access
    - Equipment handover
- Incident Reporting
    - Security reports
    - Lost equipment
    - Infiltration
    - Virus/Hacking
- Field Documentation and Reporting
    - Depends on methodology, but considers meta/exif data, physical exposure, mobile use, software tools, physical safety, travel

Security policy templates

- SANS security policy templates (corporate): https://www.sans.org/security-resources/policies/
- Policy used by the BBC (documents in Owncloud), http://www.bbc.co.uk/guidelines/dq/pdf/is/is_policies.pdf
- APC has a generic version that can share
- HURIDOCS has a generic version that we can share
- Linux Foundation: https://github.com/lfit/itpol
- Example of the engine room's email encryption policy: https://www.theengineroom.org/what-were-learning-about-keeping-organizational-emails-secure/