5. Security Toolkit: Security Policies

What to Include?

Security policies may cover a wide variety of topics. You should have policies dedicated to specific security topics. Below is a list of common policies needed in legal aid organizations:

- Account Management and Password policy: guidance on what kinds of passwords to use and how often to change them.
- Acceptable use policy (AUP): help staff and volunteers understand what they should and should not do with the organization's technology, systems, and data. AUP's may include requirements with respect to training, specifically security awareness training and testing.
- Remote work and remote access policies: what devices can/cannot be used; who can and cannot use a work device; how to create a secure remote environment; how to properly access organization networks remotely; and data handling practices to prevent data leakage.
- Data classification: clear descriptions of what kinds of data your organization retains and what security should be used for each kind of data. This may include which systems to use and whether/when encryption must be used.
- Data retention: schedules for how long your organization keeps data and in what forms, distinguishing between on-site data, backups, and off-site backups.
- Security breach and incident response plans: guidance on how to respond when the organization becomes aware of a possible breach (see the materials on what to do when you experience a breach below).
- Disaster Recovery Plan Policy: detailed plans on how to keep critical IT services and data available in the event of disaster and/or how to restore critical services in an acceptable time frame.
- Physical security: protect against property damage or theft by establishing rules for granting access to equipment, identifying sensitive areas, authorized personnel, the removal of equipment from the premises, and any required locks and/or video surveillance.

Security policies, like most policies, require sufficient staff and volunteer training as well as designating a role within the organization to be responsible for maintaining the policy, integrating the policy into practice, and driving compliance. Most security policies should be reviewed

annually to make sure they are still applicable, that they conform with current good practices, and that they are otherwise sufficient. There may be circumstances that arise that may call for an earlier review such as when the organization does a security assessment or suffers a security breach that highlights one or more weaknesses in current policies.

Sample Security Policies

- Company Cyber Security Policy Template
- Security Policy Templates
- IT security policies
- 30 Free IT Security Policy Templates for Businesses
