[Name] Information Security Policy Summary

Why have a security policy?

Common reasons for security breaches include reusing passwords, weak passwords that are easy to guess, or lack of multi-factor authentication. These guidelines protect individuals and organizations against most common problems.

Policy Summary

* Only use work accounts and devices for work-related business, don’t use personal accounts for work-related business.
* Use multi-factor access whenever possible
* Only grant the credentials people need to do their job
* Remove access when employees or contractors leave
* Don’t share credentials, use individual accounts
* Store important files in secure/shared locations
* Use a password manager
* Ask tech to set up new laptops for you

1: Keep work and personal information separate:

Don’t use work services for personal business and don’t use personal services for work. This applies especially to email: all business should be conducted through your work email account.

You can use personal devices to access work services, but you should not use them to store work-related information. For example, you can use your personal phone to check Slack and email, but don’t save financial statements to your personal laptop.

Why? If you leave, we want to make sure that we can still access information related to your job, while not infringing on your privacy on personal matters.

2: Use multi-factor access

We require two-factor access whenever possible for services such as Google Apps and Salesforce.

Yubikeys are available and recommended, as they are more convenient and secure than SMS or Authenticator apps. A Yubikey is available on request.

3: Only grant the credentials people need to do their job

Don’t make everyone an “admin” of all accounts. Grant people the most narrow permissions necessary for them to accomplish their job.

When someone no longer needs access to a resource, it should be revoked.

4: Remove access when employees or contractors leave

See *onboarding and offboarding policy*

5: Don’t share credentials, use individual accounts

Don’t share username/passwords. Create individual accounts whenever possible.

If you have to share credentials, use LastPass.

6: Store important files in secure/shared locations

Don’t store important information on your own device. Use Dropbox or Google Docs. Use a well-organized folder structure so other people can find your document if necessary.

7: Use a password manager

Don’t create your own passwords. Use a password manager (LastPass) to generate a unique password for each service.

8: Ask tech to set up new laptops for you

Tech will provide you with a new laptop if you need it. If you choose to use your own, bring it to tech so that they can secure it and install apps for collaborating with staff.

Version History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Modified Date | Approved Date | Approved By | Reason/Comments |
| 1.0.0 | February 2018 |  |  | Document Origination |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |