Table of Contents

Lullabot Information Security Policy

It is Lullabot's policy that the information it manages shall be appropriately secured to protect against the consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information. This information security policy provides management direction and support for information security across the organization.

This policy has been approved by the organization and forms part of its policies and procedures. It is applicable to and will be communicated to staff and other relevant parties. This policy shall be reviewed and updated regularly to ensure that it remains appropriate in the light of any relevant changes to the law, organizational policies or contractual obligations.

Leadership and Review

Policy

Lullabot will create a security team to manage and oversee its information security policy. This team should include members of management and representation from across functional areas of the company.

Scope

This policy applies to Lullabot management.

Compliance

- A team will be created.
- The security team will have a schedule of regular meetings, no less than once a month.
- A security email address will be created to allow anyone to easily contact the security team at any time.

Explanation and Implementation

The current members of the Security team include:

- Andrew Berry, Director of Technology
- Brian Skowron, President
- Ezequiel Vázquez, Senior Developer
- Sally Young, Senior DevOps Engineer
- Tim McDorman, Administrative Manager

This team is currently meeting weekly to discuss and assess security concerns. The team can be contacted at any time by sending an email to security@lullabot.com.

Access Control

Access control policies are designed to ensure authorized user access and to prevent unauthorized access to systems and services.

Virtual Private Network (VPN)

Policy

The use of a virtual private network (VPN) is required when accessing Lullabot's servers, or when accessing client's assets for clients that provide VPNs. A VPN should be always be used when working from unknown or untrustworthy locations, like public networks.

Scope

This policy applies to all Lullabot employees and contractors.

Compliance

1. Critical infrastructure assets will be available only to employees via the Lullabot VPN.
2. Since employees must use Lullabot's VPN to access some internal assets, their devices will be VPN-enabled. This will make it easy to use the VPN when they are working from any untrustworthy location.
3. Some Lullabot clients provide a VPN that is the only way that client assets can be accessed. Employees and contractors working with those clients will not be able to do their work without using the client VPN.

Explanation and Implementation

Lullabot and some of its clients provide VPNs that create secure internet connections from your computer directly to internal servers, which then forwards your traffic out to the internet. A VPN protects your traffic from being intercepted and viewed by any local network device, or even by your ISP.

It is important to understand that this only protects your traffic as it moves from your computer to an internal server. This means that once your traffic leaves the internal server, it is not any more secure than it would have been anyway. The protection is from other users or devices on your local network.

Using the VPN connection also makes all of your internet traffic appear to be coming from a Lullabot server, which means that you can connect from anywhere in the world, and as far as the greater internet is concerned, you look like you are sitting in Newark, NJ. This means that when there are access restrictions on a project, our VPN address can be added to an access control list, and you can connect from anywhere.

Finally, your VPN connection bypasses any local network restrictions. For example, it is not uncommon for public wifi hotspots to block services. By connecting to the VPN, you will automatically bypass any of these network-level restrictions. It is highly encouraged to use the VPN any time you are using public wifi at a coffee shop, airport, hotel, etc. This is especially true if you are using the same computer or other device that you use for work. If in doubt, err on the side of caution and use the VPN.

Employees can find instructions on how to connect to Lullabot's VPN at https://www.dropbox.com/work/Lullabot/VPN.

PINs, Passcodes and Passwords

Policy

Strong passwords should be used for access to any company accounts and services. We recommend creating passwords with a minimum of 16 characters and a combination of alphabetic, numeric and special characters.

Scope

This policy applies to all Lullabot employees and contractors.

Compliance

All employees and contractors are expected to create strong passwords for access to all Lullabot and client accounts.

Explanation and Implementation

The first layer of defense that we have for our online accounts is the PIN, passcode, or password. As such, it is extremely important to use good, unique passwords, and keep them well protected. A good password consists of a fully random string, the longer the better. Contrary to popular belief, the inclusion of numbers, characters, or mixed case does not matter nearly as much as the length of the password itself.

Because the human brain is not capable of remembering long random passwords, we need the help of some sort of tool, like a Password Manager.

Now that you are using one of these tools (right?), it is important to make sure that you are not using the same password on multiple services. Consider the event that one of these sites has its security compromised, and your username/password are discovered. Now, how many other places use that same combination? Are some of those important? Like maybe your email or bank accounts? This is why it is so important to use different passwords for different services.

Also, because you are now using one of these convenient tools, and would not be able to remember your passwords if you wanted to anyway, you might as well make them all super-secure. The length of a password is its primary strength. The longer it is, the stronger it is. These days, most security experts suggest passwords of 12-16 characters, minimum. But what does it matter to you if you are using copy/paste anyway? Crank those suckers up to 32 characters and be safe for the next millennium.

Finally, you should be wary of services that impose password limits, especially if they limit the length of the password. Any service that cares even a little about your security will store passwords using a well salted, secure hash which makes any password, regardless of length fit into a common length string. There is no excuse for a service to tell you that your password cannot be longer than 16 characters. If they do, they are most likely storing passwords insecurely, and if that is true, what other security protocols might they be skimping on?

Password Managers

Policy

The use of a password manager is strongly encouraged.

Scope

This policy applies to all Lullabot employees and contractors.

Compliance

There will be more requirements for long passwords, and potentially more requirements to change them. It is expected that users will require the convenience of a password manager to manage them.

Explanation and Implementation

A password manager, like 1Password, helps store and organize your passwords. With a password manager you can manage dozens of strong and unique passwords without any need to remember every one of them. Password managers store passwords encrypted. The encrypted passwords are protected by a master password, a single, very strong password which grants the user access to their entire password database. This master password could be a phrase instead of a single word to make it longer and harder to guess.

Some password managers include a password generator that can automatically generate very strong passwords for each of your accounts. This makes it easier to create the long, complex passwords that keep your accounts safe.

Many password managers make it possible to share passwords across devices, so you could store the passwords once, then use them on your computer, your tablet, and your phone. Many also include provisions to share passwords with colleagues or family members. Additionally, they often include features like 'secure notes' where you can store other information securely, like fallback passcodes for accounts that were set up using two factor authentication.

A password manager can compare the current site's URL to the stored site's URL. If the two don't match then the password manager should not automatically fill in the login fields. This would be a safeguard against visual imitations and look-alike websites. Many of the better password managers handle multi-page fill-ins, and multi-factor authentication as well.

In contrast to password managers, there are more simple password syncing services built into most common web browsers, like iCloud keychain and Chrome's built-in password management. These services store passwords, and may sync them across devices, but they're browser-specific, and they don't have additional features like password generators. In fact, if you are using a password manager, you don't need password syncing, and you could disable these services and delete their stored passwords to avoid potential confusion from having multiple services storing passwords and trying to auto-populate your password fields.

Two-factor Authentication (2FA)

Policy

Two-factor authentication (2FA) is required for any account or service that supports it, if that service provides access to Lullabot or client information. This includes, but is not limited to, Gmail, GitHub, Dropbox, and Slack. Lullabot employees and contractors will need to set up 2FA to log into these accounts.

Scope

This policy applies to all Lullabot employees and contractors.

Compliance

1. No less than once a year, all accounts and services that provide access to Lullabot or client information will be reviewed to determine if 2FA is available, and, if so, ensure the service has been configured to require 2FA.
2. When new accounts or services are added, they will be configured to require 2FA, if 2FA is available.

Explanation and Implementation

Traditional authentication consists of a username and password. However, there is a more secure way to authenticate, called two-factor authentication. Two-factor authentication consists of something you know (a username and password) combined with a code available from something you have. The "something you have" is usually another device, like your phone.

When logging into an account that has been set up with two factor authentication, you will be asked for your username and password as usual, but you will also be asked for the *current* PIN.

There are several ways to generate this PIN. It could be sent to the phone as a text message or email. Or you could install an authentication app. Examples of authentication apps are Google Authenticator or Authy. When an authentication app is linked to your account, the app will display a six digit PIN that changes once every minute. Using an app is great for those moments where your laptop has internet access but your phone doesn't have a signal to get a text message.

Two-factor authentication is significantly more secure than single-factor (username and password only). If someone figures out your single-factor authentication credentials, they can access your account indefinitely without you knowing, or worse, log in and change your password to lock you out. With two-factor authentication, there is a time-based token that they would need to know, too, and it continuously changes. This keeps your account much more secure.

You should be sure you have some way to recover access to your account if your phone is lost or destroyed. Most Lullabot-run accounts can be reset by an admin, but it can be problematic for personal accounts or smaller services without group or company features. An easy way to think about it is to think about how you would recover from a (local) disaster like a fire or flood. If you lost every piece of technology you owned, could you recover your accounts? Some strategies include:

- Google lets you specify multiple recovery phone numbers. Set up SMS fallbacks to your own phone or to another trusted person. You can always get a new phone or SIM card for your own number. PINs sent to other numbers won't compromise your accounts unless they also know your logins and passwords.
- The Authy app provides an option to share codes across devices. This would allow you to retrieve your code from some other device that has the app installed.
- Print out 2FA recovery codes and store them securely outside of your house.

- Store recovery codes in the notes field in 1Password if it's accessible from multiple devices. However, if you choose to optionally enable 2FA for 1Password itself, store a hard copy of the recovery codes securely.
- Determine if the service will let you recover an account with proper government ID. For example, Linode will do this, while GitHub will not.
- Determine if an account can be reset by an account admin - Google Apps accounts can do this, while GitHub and others can not.
- Do not store recovery codes in unencrypted services like Dropbox or iCloud.

Shared Passwords

Policy

Shared passwords shall be managed in a central application, where access can be monitored and passwords can be easily changed.

Scope

This policy applies to all Lullabot employees.

Compliance

- Shared passwords will be managed using 1Password vaults.
- Separate vaults will be created for groups of passwords that should allow access to the same group of people. Permission will then be set at the group level.
- Shared passwords will be changed whenever employees leave Lullabot, or if there is any reason to be concerned that shared passwords may have been compromised.

Explanation and Implementation

1Password has many advantages for managing shared passwords:

- Provides easy access to a password manager that can be used for other passwords.
- 1Password Business includes a free 1Password Families membership for everyone in your company. Multiple accounts make it easy to separate personal data from business data, and at the same time see everything you need on all your devices.
- This does not change anything for non-1Password users, just where they find the shared password.
- 1Password does not have access to our passwords.
- The 1Password plugin works in Safari.
- If 1Password goes offline, we can still access our vaults locally.
- 1Password has group-based sharing permissions.
- 1Password provides an analysis of password strength.
- 1Password has event logging, which will show who accessed/changed a password, when, and from where.
- Passwords are accessible with no software installation.
- 1Password supports a variety of 2FA options.
- Users of other password managers probably want to make a few adjustments if they want to continue using their own password manager for their personal accounts:
- Consider using separate browsers for work and personal.
- Consider using web-access to 1Password instead of the extension.
- May be able to configure 1Password to not ask about saving passwords.

Recommendations for users

In your Lullabot account, do not store personal, non-Lullabot related passwords. Create a personal account and link it to the shared account.

- This is even 1Password's official recommendation.
- Admins can reset and lockout Lullabot 1Password accounts. Admins ultimately can get access to its contents.

- Termination from Lullabot will at least result in loss of access to your Lullabot account, and at most will result in irrecoverable loss of the data in that account.

Shared Accounts

Policy

Shared accounts will not be used on systems that have the capability for individual user accounts.

Scope

This policy applies to all Lullabot employees and contractors.

Compliance

- Individual accounts will be used for all services that support them.
- If a service does not support multiple accounts, access credentials will be stored in the shared password manager with access only granted to the users who need it.
- Written confirmation from a client is required if the client requires use of a shared account in a service they manage.
- When comparing multiple services, services that support individual accounts will be preferred over those that do not.
- Invitations to services should be sent by email address, and not user name, to avoid inviting wrong members to a team.

Explanation and Implementation

While shared accounts offer simplicity compared to maintaining individual accounts, they make other security objectives difficult or impossible to meet. Shared accounts:

- Do not identify individual owners of work products.
- Do not provide an audit log that allows relating an action to a named individual.
- Do not allow for offboarding of a team member without rotating and redistributing credentials.
- Do not allow for proper notifications in communication tools, such as mentions in issues or tickets.

Most services aimed at teams offer per-user accounts, such as GitHub, Drupal.org, and Jira. However, "infrastructure" services such as domain registrars often only support a single account.

Some services, like GitHub, allow for a single identity to have multiple attached email addresses, such as a personal and a work email. Team members may use existing personal accounts for services like these, however they must attach a Lullabot email address to the account. All invites and other onboarding activity should be done by email address and not user name to ensure that invitations are not sent outside of the organization.

Physical and Environmental Security

The goal of physical and environmental security policies is to prevent unauthorized physical access, damage and interference to the organization’s information and information processing equipment.

Acceptable Use Policy

Policy

This Acceptable Use Policy (AUP) for information systems is designed to protect Lullabot, our employees, customers and other partners from harm caused by the misuse of our information systems and our data. Misuse includes both deliberate and inadvertent actions.

The repercussions of misuse of our systems can be severe. Potential damage includes, but is not limited to, malware infection (e.g. computer viruses), legal and financial penalties for data leakage, and lost productivity resulting from network downtime.

Scope

This policy applies to all Lullabot employees and contractors.

Compliance

Everyone who works at Lullabot is responsible for the security of our information systems and the data on them. As such, all employees must ensure they adhere to the guidelines in this policy at all times. Should any employee be unclear on the policy or how it impacts their role they should speak to their manager or IT security officer.

Lullabot will not tolerate any misuse of its systems and will discipline anyone found to have contravened the policy, including not exercising reasonable judgment regarding acceptable use. While each situation will be judged on a case-by-case basis, employees should be aware that consequences may include the termination of their employment.

Use of any of Lullabot's resources for any illegal activity will usually be grounds for summary dismissal, and Lullabot will not hesitate to cooperate with any criminal investigation and prosecution that may result from such activity.

Acceptable Use

Lullabot's systems exist to support and enable the business. Personal use is allowed. However it must not be in any way detrimental to users own or their colleagues productivity and nor should it result in any direct costs being borne by Lullabot other than for trivial amounts.

Any information that is particularly sensitive or vulnerable must be encrypted and/or securely stored so that unauthorized access is prevented (or at least made extremely difficult). However this must be done in a way that does not prevent–or risk preventing–legitimate access by all properly-authorized parties.

Lullabot can monitor the use of its IT systems and the data on it at any time. This may include (except where precluded by local privacy laws) examination of the content stored within the email and data files of any user, and examination of the access history of any users.

Lullabot reserves the right to regularly audit networks and systems to ensure compliance with this policy.

Users must take all necessary steps to prevent unauthorized access to confidential information. Users are expected to exercise reasonable personal judgment when deciding which information is confidential.

Users must not send, upload, remove on portable media or otherwise transfer to a non-Lullabot system any information that is designated as confidential, or that they should reasonably regard as being confidential to Lullabot, except where explicitly authorized to do so in the performance of their regular duties.

Users must keep passwords secure and not allow others to access their accounts. Users must ensure all passwords comply with Lullabot's safe password policy.

Users are responsible for the safety and care of electronic equipment, and the security of software and data stored it and on other Lullabot systems that they can access remotely using it.

Because information on portable devices, such as laptops, tablets and smartphones, is especially vulnerable, special care should be exercised with these devices, including encrypting computers, and using strong and secure passwords and pins. Users will be held responsible for the consequences of theft of or disclosure of information on portable systems entrusted to their care if they have not taken reasonable precautions to secure it.

All workstations (desktops and laptops) should be secured with a lock-on-idle policy active after at most 10 minutes of inactivity. In addition, the screen and keyboard should be manually locked by the responsible user whenever leaving the machine unattended.

Users who have been charged with the management of those systems are responsible for ensuring that they are at all times properly protected against known threats and vulnerabilities as far as is reasonably practicable and compatible with the designated purpose of those systems.

Users must at all times guard against the risk of malware (e.g., viruses, spyware, Trojan horses, rootkits, worms, backdoors) being imported into Lullabot's systems using best practices for the operating system in use, and must report any actual or suspected malware infection immediately.

Unacceptable Use

All employees should use their own judgment regarding what is unacceptable use of Lullabot's systems. The activities below are provided as examples of unacceptable use, however it is not exhaustive. Should an employee need to contravene these guidelines in order to perform their role, they should consult with and obtain approval from their manager before proceeding.

- All illegal activities. These include theft, computer hacking, malware distribution, contravening copyrights and patents, and using illegal or unlicensed software or services. These also include activities that contravene data protection regulations.
- All activities detrimental to the success of Lullabot. These include sharing sensitive information outside the company, such as research and development information and customer lists, as well as defamation of the company.
- All activities that are inappropriate for Lullabot to be associated with and/or are detrimental to the company's reputation. This includes pornography, gambling, inciting hate, bullying and harassment.
- Circumventing the IT security systems and protocols which Lullabot has put in place.

Device Lock Screens

Policy

Device lock screens should be configured to prevent access by unauthorized users, or when lost or stolen.

Scope

This policy applies to all Lullabot employees and contractors.

Compliance

All Lullabot employees and contractors are required to protect all devices in their possession that have configurable locking options.

Explanation and Implementation

The pins or passwords used to unlock devices deserve special mention. They are literally the "keys to the kingdom", especially for mobile devices that are easily lost or stolen.

The password used to unlock a computer should be a strong, alphanumeric, password.

Phones often default to a simple 4-digit pin. That is too weak to be effective, so a longer, stronger pin should be used.

On Android, choose a more unpredictable pattern or create a longer PIN (up to 16 digits).

On iOS, go beyond the standard four-digit PIN by going into Settings >> Touch ID & Passcode >> Change Passcode. When setting the new passcode you will see a link called "Passcode Options". You can select that to choose either an alphanumeric passcode or a longer numeric passcode.

In addition, devices should be configured to lock automatically after a short period of inactivity, and they should be locked manually any time the owner walks away from them.

Hard Drive Encryption

Policy

All computer hard drives should be encrypted.

Scope

This policy applies to all Lullabot employees and contractors.

Compliance

All Lullabot employees and contractors are responsible for encrypting any machines in their possession.

Explanation and Implementation

As a client services company, we often are forced to store sensitive client data such as user information or other proprietary commercial data. While we're insured for this type of data loss by our Technology Errors and Omissions insurance we should do everything in our power to make sure data loss is never an issue we have to confront. One of the most important steps you can take is the encryption of your hard drive. This ensures that if your computer is lost or stolen, the thieves will be unable to access the information stored there. For macOS users, FileVault is generally enabled by default. Confirm that it is by following Apple's instructions. If you're on Linux or Windows, please take similar measures to enable full-disk encryption with BitLocker or an equivalent. Note that Bootcamp on Macs does not support disk encryption at all. If you must use Bootcamp for Lullabot work, create an encrypted disk image with BitLocker or Veracrypt and install portable apps to keep the data secure.

Backups

Policy

All computers must be backed up regularly, and backups must be encrypted.

Scope

This policy applies to all Lullabot employees and contractors.

Compliance

All Lullabot employees and contractors are responsible for backing up any machines in their possession.

Explanation and Implementation

Backups are by far the most overlooked or ignored, and arguably one of the most important parts of a computer system. They are overlooked because they are boring and provide no immediate benefit. But, when disaster hits it is too late. If you do not have backups then you are in trouble.

There are multiple levels of backups, each with their own merits and costs. These levels range from keeping a copy of a file in a different folder on your computer all the way up to fully automated, full disk backups to the Cloud. Which level is appropriate depends on the data in the backup, and ultimately how you answer the following question:

What would I do if my working copy of this data disappeared?

For many of us at Lullabot, much of our work lives on GitHub, Google Drive, Dropbox, or some other online service. In this case, our answer might be "I would download a new copy" or "I would revert to a previous revision" or "I would contact service X and ask them to restore the data" and that might be enough. Nevertheless, in the likely case that this is not enough, a backup strategy is in order.

Time Machine on macOS makes automated backups very easy with an external hard drive. This should really be considered the baseline backup level for your computer. Turn on Time Machine, and for the most part just forget about it and let it run. Even if most of your work is online, having Time Machine backups makes replacing a machine a much easier task. Instead of spending hours reinstalling applications and setting up preferences, you can start the restore process and come back to a ready-to-use machine.

Remember, it’s important to enable encryption for your Time Machine backups, just as you do with your hard drive. This is enabled by default in recent macOS releases. If for some reason encryption is disabled, you can enable it with:

- Go to System Preferences >> Time Machine
- Select “Stop using for backups”
- Then “re-add” and when you do, select “encrypt backups”

Now that you feel all warm and fuzzy about being protected from accidental data loss on your computer, think about what you would do if both your computer and your backup device were stolen or destroyed in a fire, flood, or worse? What would you do? Could you get a new computer and get back to work? Probably to some degree, but would you be missing some important files? Most likely.

A second layer of backups to an off-site location is the only way to protect yourself from this type of data loss. There are different ways to approach this problem, too, such as shipping a copy of your Time Machine volume to your parents every so often, or finding a friend to host an FTP server that you can dump files to every so often. These

strategies are not wrong, but there are more practical solutions involving cloud storage. The simplest solution would be to store all of your important items in a Dropbox folder, though Dropbox is not a real backup solution. You could subscribe to a cloud backup service, but note that most services like Backblaze and Carbonite don't have appropriate encryption support for Lullabot data. These services are relatively cheap and may prove an important form of insurance. For a cheaper but slightly more complicated option, consider setting up Amazon Glacier storage with Arq for your encrypted backups. Reach out to the team in on Slack in `#apple`, `#linux`, or `#windows` to find out about current tools and best practices.

Lost or Stolen Devices

Policy

Reasonable steps should be taken to ensure that devices that contain or provide access to Lullabot information won't be compromised if lost or stolen.

Scope

This policy applies to all Lullabot employees and contractors.

Compliance

Encryption and secure screen lock pins are the first line of defense against compromised security from lost or stolen devices. 'Find my [phone|computer]', and remote wipe features can also be enabled for additional protection.

Explanation and Implementation

What happens if your device is lost or stolen? The best scenario is where you can recover it and ensure that no one else could have accessed data on it, since you have a screen lock and encrypted your disk. The next best is where you can recover your device, without knowing if anyone accessed or changed files on it. For example, if your disk isn't encrypted, someone could have easily installed a keylogger to siphon off passwords. The worst scenario is where you completely lose an unencrypted device. In that case, you should assume everything is compromised and start resetting and recovering accounts.

To prevent problems:

- Make sure all computers and phones have encryption enabled.
- Create secure pins and passwords for device screen locks.
- Enable Find My Phone|Computer features, where available. For Apple devices, at least, this includes options to remotely wipe a lost or stolen device.
- Consider adding contact information to your lock screen to make it easier for someone who finds your device to return it.
- Consider enabling the emergency contact info on your phone.

Also make sure that you have strong passwords for any accounts that can remotely wipe devices. Individuals have been targeted by remote wiping their devices through weak iCloud passwords, making it very difficult to recover accounts.

Android Devices

Android Device Manager is the easiest way to find and manage Android devices. Your phone manufacturer (Samsung, Motorola, etc) may also have device recovery software you can use. ADM lets you locate, ring, and erase devices. You can also set up a new lock screen code.

It's also a good idea to put contact information on your phone's lock screen. In Android 5, it's under Settings -> Security -> Owner info, and is available in older Android versions as well. Make sure your contact info isn't only accessible on your phone!

iOS and Mac Devices

For an Apple device, there's a handy tracking utility that can help you either locate the lost device, or, in the event of a theft, wipe the device's memory so that your data is safe. Part of the iCloud services offered by Apple includes the "Find My iPhone" app available for iOS devices and on MacOS.

On iOS, visit Settings >> iCloud and make sure you turn on "Find My iPhone". Next, download the Find iPhone app that's free from the app store so you can view your devices on a map. This app will also allow you to remotely wipe a device that is no longer safely in your possession. If your device is stolen, you may also be able to see where the thief has taken it.

On the Mac, go to System Preferences >> iCloud and make sure you enable the "Find my Mac" option so that your desktop machine will also be protected in this manner.

The Apple support site has more information about how to use Find My Phone and Find My Mac features.

On both iOS and OS X you can put contact info on the lock screen. For OS X, it's under "Security & Privacy" in System Preferences. Make sure your phone number or email isn't only accessible on your phone!

On iOS you can use an app to burn info into an image. If the phone is lost you can also display contact information on the lock screen of the lost device using the "Find My iPhone" screen in iCloud.

Add emergency contact info to your phone

Finally, you can add emergency contact information to your phone. Emergency information is accessible on a locked device, and will provide an additional way for someone to find the owner of a device.

What to do when you've lost a device

Figuring out appropriate next steps for this can be pretty complicated. As well, being distributed makes us an easier target for impersonation attacks. We should assume we are not concerned about nation-state level attacks; if Chinese sponsored attackers try to get into a client (think Sony and North Korea) through us, we're probably subject to zero-days and the like.

Finding your lost device is the first step to figuring out how much you need to do to make sure everything remains secure.

Is there a realistic security issue, or just a lost device?

The first step is to figure out if it's reasonably possible for someone to get access to accounts and data from the lost device. Laptop drives are accessible if they aren't encrypted. Encrypted devices are accessible if they aren't locked. If a laptop is stolen and we can't know if it was locked, we should assume the contents are open to the world, as all it takes is a (cheap) USB device to keep it awake. If someone isn't sure, they should reach out to the hive-mind for advice. A smart attacker will also keep LastPass or 1Password unlocked.

You lost a device that was encrypted and locked or off:

You probably don't need to do anything security-wise other than letting the team know you lost your device.

You lost a device that might have been unlocked, but you store passwords in a password manager that was known to be locked:

You don't need to reset passwords or credentials except for anything that might be in plain text. If you have apps that don't use the OS X keychain, you might need to reset those credentials. Windows and Linux apps commonly store passwords in clear-text (or mildly obfuscated) on disk. API tokens should be reset, like those used by Composer for GitHub access or those stored in settings.php in client sites.

If you get your device back, assume it's been compromised with a keylogger. Wipe it and restore it from a known-good backup. This includes ignoring any potential cloud backups made since you lost the device.

You lost a device without encryption (a Windows laptop, a Time Machine backup drive, an Android phone)

Post to Yammer to let the team know you lost a device. The team should take this as a note to be on guard for suspicious activity. If you lost *all* your devices, call 1-877-LULLABOT or your manager.

Get on a phone or video call with a member of the admin team to confirm the lost device. **Managers and the admin team should not accept text communication as proof that they are communicating with an employee**. Confirm with them what accounts you need them to reset. They should be able to reset passwords quickly for Lullabot-managed accounts like Google Apps and the Daily Report. If warranted, the admin team should send an email to team@lullabot.com alerting the company about the lost device.

After regaining access to your Lullabot email address, use it to reset passwords for accounts to log out all active sessions. Some services will let you log in, list, and kill active sessions, saving you from having to reset your password.

High-profile services to have an admin team member immediately reset or log out all sessions if you can't do it yourself:

- Google
- Daily Report / LDAP
- Bamboo HR
- Linode Manager
- Slack
- Yammer
- Noko

Services individuals need to reset or log out on their own once the above is done:

- GitHub
- Client-specific services (like Jira, Hipchat, etc)
- Drupal.org
- Twitter, Facebook, etc

Commonly forgotten items:

- API keys for services in code
- Passwordless SSH Keys
- Backup services like CrashPlan, Carbonite, and so on

Data loss and client notifications

Talk with your manager to figure out what actions are appropriate for any client code or databases on your device. Remember to consider past clients who you might not be actively working for at the moment. If there were database dumps on your machine that weren't encrypted or sanitized, follow the same steps as if a production or development environment had been compromised. Deleted files can still be recovered from unencrypted drives.

Malware and Viruses

Policy

Lullabot employees and contractors are expected to adhere to best practices for avoiding malware and viruses.

Scope

This policy applies to all Lullabot employees and contractors.

Compliance

Each employee or contractor will be responsible for their own equipment.

Explanation and Implementation

Protection against malware and viruses includes, but is not limited to:

- Avoid installing unlicensed software, pirated music, video, software, these can be a vector for malware.
- Protect devices from malware and viruses by enabling the firewall and using virus protection software.
- Use an ad-blocker. The business model for ad networks is contrary to best security practices, making them easy targets for hackers.
- Make Flash and Java click-to-play, Choose “Ask” rather than the default of “Allow” in Safari.
- Install ClamAV and have it scan folders with user uploaded data.

Ad-blocker configuration

uBlock Origin is the most commonly used "content blocker" for web browsers. Chrome and Firefox are officially supported, and there are ports for other web browsers too.

Installation links

- Chrome
- Firefox
- Edge
- Safari

The out-of-the-box configuration of uBlock is very good. Feel free to customize settings, but it's not required. The toolbar button can be used to disable blocking on a per-site basis, which is useful when working on client sites or visiting sites that have committed to auditing and securing their ads.

For further security and control, consider using an extension like NoScript or Ghostery.

Ransomware

Lullabot employees and contractors should watch for ransomware attacks, as companies are often targeted by such scams. Ransomware is a specialized variant of malware, where documents and data are encrypted using strong cryptography. Then, the malware will attempt to extort a fee for a "recovery key" out of the business. Ransomware is distributed through a variety of means, including compromised websites and advertising servers or email. Most Ransomware will attempt to encrypt all accessible documents, including those on network or external drives.

Lullabot has a general policy of not paying attackers to unlock files. Instead, we treat ransomware just like any other disk failure. If you are infected with ransomware, wipe your disks and recover your data from backups and from the cloud.

The following types of backups may be at risk from a ransomware infection.

- *Time Machine backup disks*: Employees should have a second backup system (such as an off-site cloud backup) that protects their data if the Time Machine backup is unusable. This second backup should not be "mountable" as a normal file system, and should have it's own server-side versioning to protect data.
- *Files synced to your computer from cloud services*: This includes services such as Dropbox, iCloud, and Google Drive. We rely on Dropbox's restore features to protect these files.
- *Network drives*: NAS appliances should have snapshots and off-site backups. For example, a Synology NAS with BTRFS protects against ransomware from a network mount by not exposing the snapshots to network users.

Source code is typically not vulnerable to ransomware as server-side version control (like Git) protects the code.

Device Maintenance

Policy

Lullabot employees are expected to adhere to best practices for maintaining any devices in their possession.

Scope

This policy applies to all Lullabot employees.

Compliance

Each employee will be responsible for their own equipment.

Explanation and Implementation

Best practices for maintenance of electronic equipment includes, but is not limited to:

- Use surge protectors.
- Enable the firewall.
- Procure insurance to cover potential equipment loss or damage.
- Maintain a regular backup schedule.
- Remove or disable the guest account on a laptop.
- Disable options to share the hard drive.
- Consider using a separate router and SSID for personal and IoT network connections.

Unlicensed software, pirated music, video, software are not permitted on Lullabot laptops, these can be a vector for malware. They can introduce vulnerabilities and lead to information leakage, loss of integrity and other information security incidents, or to violation of intellectual property rights.

Asset Inventory

Policy

All computers and cell phones will be tracked in an inventory management system.

Scope

This policy applies to all Lullabot employees and management.

Compliance

- Whenever a new computer or cell phone is purchased, details about the asset will be entered into an inventory tracking system.
- Whenever a computer or cell phone is taken out of service it will be removed from the asset tracking system.
- The system will track identifying information, including make, model, and serial number.
- The system will track the location of the item and identify the person who has possession of it.

Explanation and Implementation

Lullabot tracks assets and equipment in an inventory tracking system. All computers and cell phones used for Lullabot business will be tracked in this system, regardless of who purchased them or when they were purchased.

PEX and Other Purchases

Whenever a computer or cell phone is purchased with PEX or Lullabot funds, details about the asset will be entered into the inventory tracking system by administrative staff when they process the receipt. The purchaser can add the serial number and other information as a comment to the purchase in the PEX system.

If the asset is replacing an older piece of equipment, the older equipment should be removed from service at that time. The administrative staff will be responsible for determining when this should be done and following up with the person who has control of the older asset.

Removing Assets From Service

Computers and cell phones that have been replaced, or those which are being sold to employees, should be properly removed from service.

- All Lullabot or client data should be removed from the device.
- All Lullabot and client passwords, pins, and password managers should be removed or emptied.
- If it's impossible to identify and separately remove such data, the device should be wiped and restored to factory defaults.
- Once sensitive information has been removed from the device, it should be deleted from the asset inventory.

Asset Inventory

Asset inventories shall be conducted periodically. At that time details about computers not already in the asset management system can be added, and computers no longer in service can be removed from the system.

An initial inventory shall be performed to collect an accounting of computers and cell phones purchased prior to the time when this policy was implemented.

Communications

The goal of communications security policies is to maintain the security of information transferred within an organization and with any external entity.

Email Security

Policy

Employees and contractors should be aware of the security implications of email communication, for instance:

- Users should be aware that email may not originate from the person it purports to come from and use care in responding to it.
- Sensitive information like passwords and IDs should not be communicated by email.
- Avoid sending sensitive files as email attachments.
- Share Dropbox files using Dropbox's recommended protocols.

Scope

This policy applies to Lullabot employees and contractors.

Compliance

Each individual is expected to use caution in any email they initiate or receive, and help monitor and remind others of potential security vulnerabilities of any email threads they are included in.

Explanation and Implementation

Avoid sending sensitive information in email, including:

- Passwords
- Server credentials
- Private keys
- Government issued IDs (Social Security numbers, etc.)
- Other private credentials or IDs

Secure methods for communicating sensitive credentials or information include:

- Using a shared vault in 1Password.
- Verbally exchange information on video or phone.
- In BambooHR for HR-related confidential information.
- For clients without a password manager or the expertise to use encryption, use 1Password links to manage items and their access.

Be conscious of the fact that email might be intercepted or viewed by people other than the intended recipients, so don’t attach sensitive files to emails.

Dropbox is a secure way to share some types of information, but be aware of the best ways to use it:

- Use Dropbox's file sharing protocol to control access to files and folders that need to be shared, and to share them securely.
- Dropbox links may be accessible by anyone who has the link, so use the "share" process rather than copy/pasting Dropbox links in email.
- Note that Dropbox allows things to be shared ‘read-only’. Use the principle of minimum required access and only offer write access if required.
- Consider encrypting the files before uploading them to Dropbox. Dropbox does not provide meaningful encryption of files by default.

- For clients and external vendors without their own solutions, Dropbox File Requests can be used to ask for files.

Everyone should be aware that email they receive may not originate from the source it purports to come from. A common threat is phishing, an attempt to obtain sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity. All email requests for sensitive information should be verified independently, not by using links or phone numbers included in the email, but instead using previously-vetted contact information to call or contact the person to confirm the request.

Security in the Cloud

Lullabot permits the use of public cloud applications, tools and technologies, known as “cloud services”. However, the use of insecure cloud services can introduce unintended risk to you, your coworkers, and the company. We want to balance the security of our content, networks and applications with the ability to work in a flexible, productive environment.

What is a cloud service?

We consider a cloud service to be any software as a service application that is hosted by the software vendor. The Google Suite, Dropbox, and Noko are all cloud services. As a distributed company working with many clients, cloud services make our business possible in the first place. Some applications may not seem like cloud services, but use the cloud for sync and storage. For example, Apple Music is a cloud service, even though it’s only accessed through iTunes and not a web browser.

What needs to be done to introduce a new cloud service at Lullabot?

Read the following, and then fill out the service request form.

If a new cloud service is purchased individually on PEX, and it does not require integration or access to Lullabot data stored in other services, no specific approval is required. Examples of services like this include:

- Evernote
- Arq Cloud Backup
- Microsoft Office 365

Be wary of applications that use your Lullabot account to access key personal data like email, especially if they are free or are low cost.

Apps that integrate with services used by the Lullabot team or interact with Lullabot customers should be discussed with the relevant directors and also need review by the security committee. Since these services are used by multiple team members, and not individuals, they typically are charged to a Lullabot expense card or are invoiced. Examples of services like this include:

- Geekbot, as it requires integration with our Slack instance.
- Drift, as it interacts with Lullabot customers and gathers their personal information.
- CircleCI, as it has access to customer owned source code.

Where possible, clients should be the account owner of cloud services in client engagements. While the security committee can provide feedback, the client should be primarily responsible for how they want to handle security reviews, if any.

When do I use my Lullabot email and when do I use my personal email when signing up for Cloud services?

- If you are signing up for a service paid for by Lullabot, or a Lullabot client, use the Lullabot email address.
- If you are signing up for a service at the request of Lullabot, or a Lullabot client, use the Lullabot email address.

- If you are signing up for a service that will contain or provide access to Lullabot data, or Lullabot client data, use the Lullabot email address.
- If you are signing up for a service that you would continue to use even if you were no longer employed at Lullabot, use your personal email address.
- If you are signing up for a service that will not contain or provide access to Lullabot data, nor be used by others at Lullabot or Lullabot clients, use your personal email address.

If a service supports multiple email addresses per account, it's OK (and even recommended) to use one "account" with multiple "identities". GitHub is the most notable example of this, though services that are built on top of GitHub likely use the same model. For example, instead of creating a new account, add your Lullabot email address to your existing account. Use the built-in tools to associate work and personal email addresses with the right organizations and projects.

Some clients will create email addresses for you. Where possible, use your Lullabot email address instead of a client email address. This is especially important for VPN recovery, where client email may not be accessible outside of the VPN. Consider redirecting your client email to your Lullabot email if it's supported by the client.

There are times when the answers might conflict, and you could make a case for using either email address. When in doubt communicate with your manager or the security team for instructions.

How should I invite users to a Cloud service?

Many services can identify accounts with either a user name or an email address. If a service offers both (like GitHub), add accounts with person's email address rather than their username. That way, a typo in the invite is less likely to add someone completely unknown, and is more likely to be scoped to just accounts at the company you are working with.

What if there are both personal and business versions of a cloud service?

Many cloud services used by Lullabot include provisions to store both business and personal information. For instance, there is a Lullabot Dropbox account, but you can also establish a personal Dropbox account and link them together. Our 1Password Business membership includes a free 1Password Families membership for each employee.

Any time there is an option to separate personal and business data in the cloud, we require employees to respect that separation. Don't put Lullabot data, or Lullabot client data, into your personal account, nor add personal information into the Lullabot account. Lullabot won't ever have access to your personal account, so nothing that belongs to the company or its clients should go into it. The test for whether you have separated your personal data properly is to confirm that if you were to unexpectedly lose access to the Lullabot account, you would still retain all your own personal data.

Some services, like iCloud, provide no easy way to separate business and personal data. Since company data is involved, we require that you use best security practices to protect all the data stored in these systems. These best practices include storing the data in encrypted format, and using encryption when transferring data by using HTTPS and the VPN as appropriate.

How do I know it's safe to use a cloud service?

The security team follows these guidelines when evaluating a new service. For example, when we investigated using Bamboo HR for Lullabot, we reviewed their Terms of Service, Privacy Policy, and any Security Policies. Examples of what was checked include:

- Their site HTTPs configuration with SSL Labs
- Their policies for data encryption and backup
- Their policies for who at BambooHR had access to our HR data
- Their password and password recovery policies (such as, do they limit passwords to 12 characters, or only allow letters and numbers)
- Their account and data deletion policies
- Their security reporting and notification practices

A search for “breach” or “leak” is also a good test to see if a service has a record of poor security. Instead of just investigating if a given service was breached, investigate how they handled the breach and how their systems were designed. For example, Yahoo has been shown to have a poor security track record, storing personal data and passwords in a way that made it easy for attackers to exploit.

Consider the type of data you are using the cloud service for. If all they have is your name and email address, the risk is pretty low. Don’t use client data when trying out a new service, so if it does turn out to be insecure, the breach is limited. This also applies to service access tokens and API keys (e.g. a Pantheon Terminus token or a GitHub API key). These should not be used with cloud services such as hosted development environments like GitPod. Tokens can be added to CI services, but they should be as tightly scoped as possible and not allow cross-client access. For example, don't generate a Pantheon access token from your personal user account which has access to multiple clients. Instead, create a bot user for that specific project and tie all tokens to the bot.

In general, the security team aims to provide feedback on possible issues to the relevant stakeholders, rather than acting as a blocker to new services. We may ask those requesting new services to help with the investigation. The fastest way to get a new service reviewed and approved is to create a document detailing the above areas of investigation.

Finally, if at all in doubt (or you just want help doing the above), ask in #security in Slack, or email security@lullabot.com.

Client Email Groups

Policy

Email related to client projects may contain sensitive information, and should be carefully controlled. Email groups shall be used to manage communications related to individual client projects. They shall be created when a project begins and archived when it ends. Employees and contractors will be encouraged to use the email lists for all client communications. Employees and contractors will remove copies of the emails contained on their computers at the end of a project, so that the archived emails under the control of the company serve as the only remaining copies of those messages.

Scope

This policy applies to all Lullabot employees and management.

Compliance

- Project or account managers will notify administrative staff when projects are initiated and when the projects end so the email groups can be created and decommissioned.
- Administrative staff will periodically review email groups to identify any that should be decommissioned, and do so.

Explanation and Implementation

Email with clients often contains sensitive information, so it must be carefully controlled. Email, by its nature, is difficult to control, since copies will be stored locally for every participant in the email message.

To better control this information, the company will create an email list for each client project and encourage employees, contractors, and clients to send email to that list when communicating about the project. The members of that list will include the staff members assigned to that project and relevant management representatives, like the account manager.

At the conclusion of a project, the email group will be decommissioned. The process of decommissioning the group will consist of:

- Sending a final email to all members of the group announcing that the group is being decommissioned and asking them to remove any copies of those emails that they have on their own computers.
- Removing all members from the group.
- Removing the option to post to the group.
- Renaming the group to a name that begins with 'ZZZ' to sort the decommissioned groups to the bottom of group lists.

At the conclusion of this process, management will still have a copy of all the messages in the group, should it be needed in the future, but all other copies of the messages in the possession of company employees and contractors should be deleted.

There will be additional benefits from directing all communications through the designated email group. Clients can easily communicate with the team without knowing every member's individual email address. In addition, new team members can be added into the group at any time, and they will have the ability to review prior communications with the client.

Slack Channels

Policy

Slack is an application used for everyday communications in Lullabot. Slack consists of a collection of channels that include a general channel and channels specific to a topic, project, or client. When these channels are no longer required, they should be archived, but not deleted.

Scope

This policy applies to all Lullabot employees and management.

Compliance

- The person who created the Slack channel will also be responsible for archiving it when no longer needed.
- Admin staff will perform a periodic review of Slack channels to identify channels that have no activity as potential candidates for archival, and contact the channel creator to confirm the course of action.
- If a client or colleague from another organization needs access to a Slack channel:
  - and they also use Slack at their organization, they will be added through the Shared Channel feature.
  - or if they do not use Slack as a part of their organization, then they'll be added using the Guest Account feature.
  - Guest accounts will be set to expire in 12 months, and renewed for additional 6 month periods as needed.

Explanation and Implementation

Slack channels can be created for specific projects and clients. These channels keep a lot of noise out of the general channel and also provide a place to talk specifically about a topic or client. Non-employees may be invited to these channels as well, allowing clients and contractors to communicate about a specific project without allowing them access to the general Lullabot channel.

The sheer number of channels makes it hard for anyone to see all the available channels and choose to join the right ones. Therefore it's useful to remove channels once the client project is finished or the topic is no longer a priority. Unneeded Slack channels can either be deleted or archived. If deleted, all communication from that channel will be lost. If archived, the communication is preserved, but the channel drops out of the list of active channels. Another advantage of archiving is that it is easy to re-activate the channel in Slack and immediately have access to the history.

Many of these Slack channels might contain sensitive or important client or project information. It's not always obvious ahead of time which information might be useful in the future. To be safe, unneeded channels should be archived, not deleted.

You can view archived channels to see or reactivate them. There are instructions in Slack about How to archive a channel. Note that private channels cannot be archived. They must be made public first, then archived.

Using PGP/GPG for Secure Communications

The original program, Pretty Good Privacy, eventually became a standard called OpenPGP. GNU PGP, or "GPG", is the most widely used PGP implementation, but for simplicity this document refers to "PGP".

PGP (Pretty Good Privacy) is a system that lets people communicate with each other securely online. PGP lets you **sign** emails and files so others can be sure they haven't been modified and are actually from you. You can also use **PGP** to encrypt emails and files so only the intended recipients can view them. Why would you want a PGP key?

- You can sign emails you send and receive encrypted email without needing to pay for a certificate. Great for passing around passwords and credentials.
- You can sign and encrypt files that can be decrypted on any computer (unlike encrypted disk images that are tied to OS X). You could use PGP to encrypt a PDF of a sensitive HR form, and then the filled-out version could have a real digital signature on the returned copy.
- If you're writing code, you can use git to sign commits and tags. That lets others verify not only that the code hasn't been modified, but that the commit by Sally Young is *actually* from Sally Young and not James Sansbury.

What are the limitations of PGP?

- Many email programs don't support any encryption systems at all, and some that do only support the centralized S/MIME standard. Most desktop email clients have plugins to add PGP support, but mobile devices usually don't support plugins in their apps.
- Using any sort of encryption or signing is difficult in webmail. Gmail can't search the contents of encrypted emails since Gmail doesn't have your decryption keys. There are browser plugins to add PGP support to Gmail on the web, but Gmail on Android and iOS don't support those plugins.
- When signing (and not encrypting) emails, recipients can get confused by the signature attachment added to the message. In general, **don't sign emails to clients** unless you know they are aware of PGP.
- For someone to decrypt a file, they have to be set up with PGP. You can't just call them and give them a password. However, PGP is pretty much the only secure solution for file encryption that works on all operating systems.

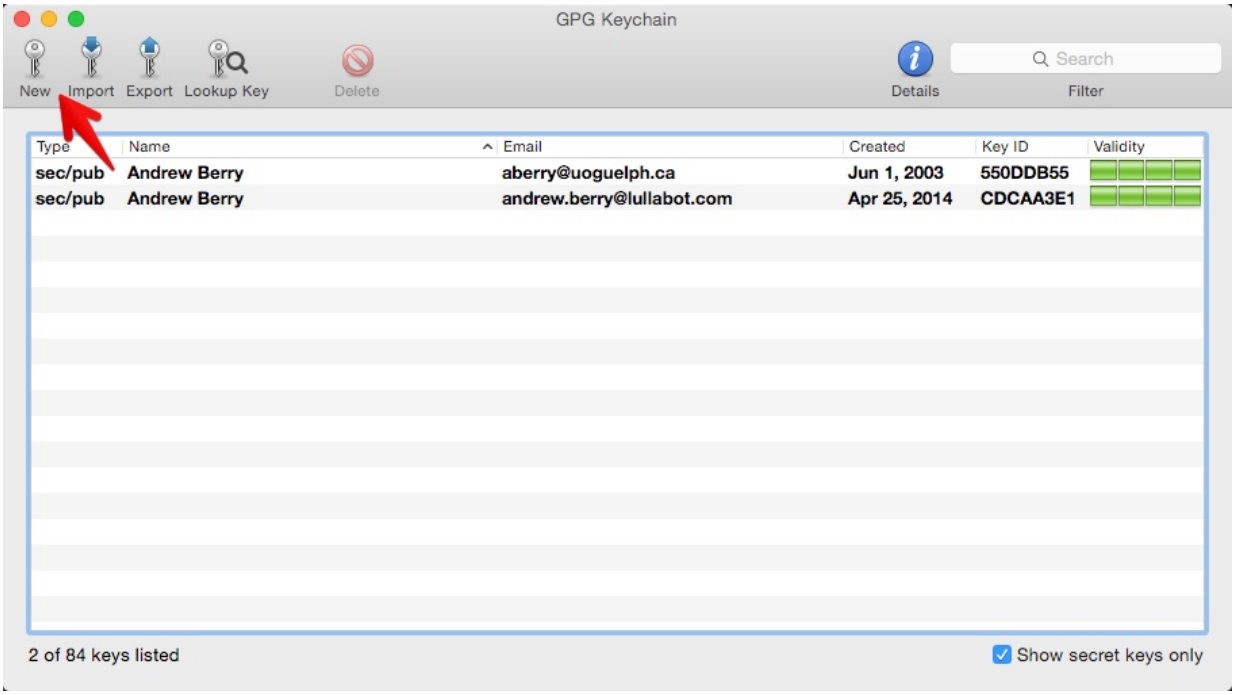
PGP uses a *web of trust* to help us validate keys and their owners. In the SSL certificate world, you pay Verisign or some other company to validate your identity. Often it's a basic email or phone call check. With PGP, Andrew can say "I validated that PGP key ASDFXYZ belongs to Matt, because I saw him in person and looked at his drivers license". If you then decide to trust Andrew's key, you'll automatically be able to trust Matt's key. This model works really well for companies like Lullabot, where we work mostly online but see each other in person a few times a year.

Creating a PGP Key

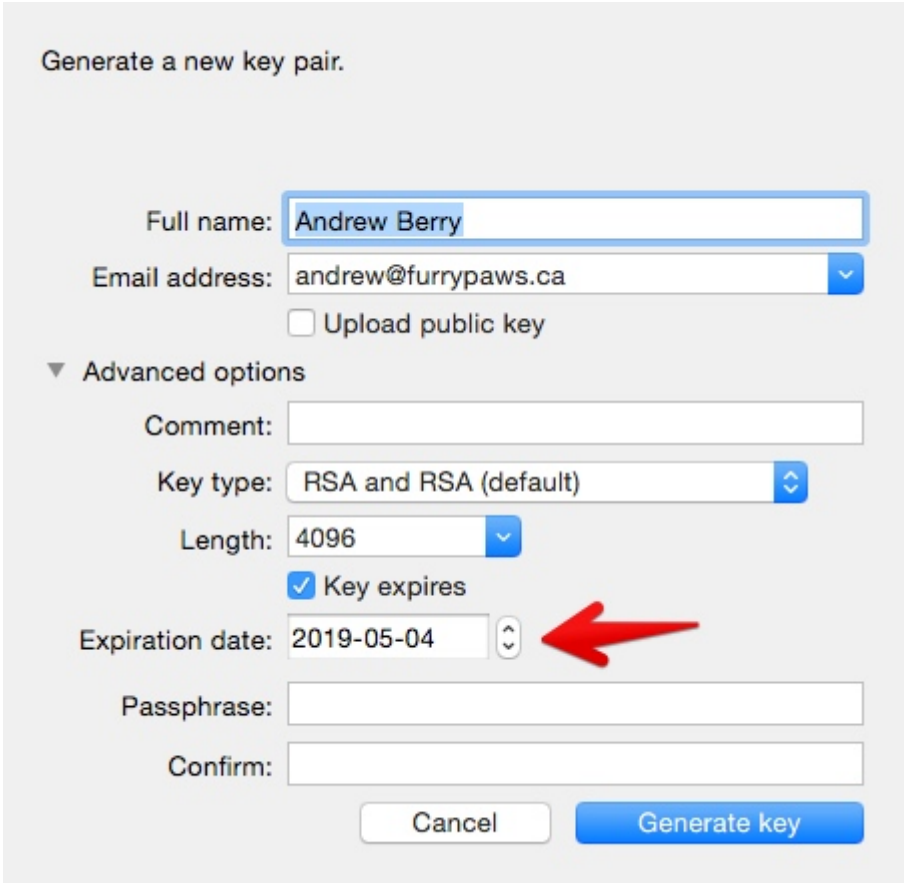
These steps use GPG Tools for OS X. GPG also has a Windows version, and is available for All The Linuxes. Every PGP key has two halves: a **public key** that you share, and a **private key** that you keep to yourself. If someone else gets your private key (or the key on your hard drive plus your passphrase), they can **pretend to be you and decrypt all your data**. Treat your private keys like you would treat your banking or Google passwords.

Create a new key with GPG Keychain

Open GPG Keychain, and click the "New" button to create a key.



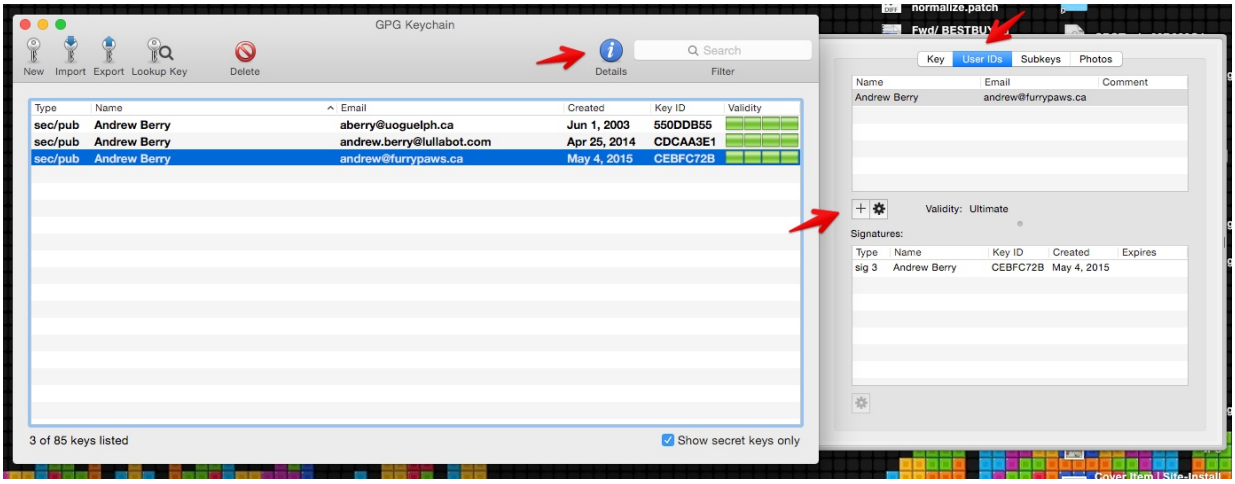
Enter your full name, and the email address you'd like to use. You can add additional email addresses later to the same key. Change the **expiration date** to one year from today. This value can be changed later, so set a calendar reminder to extend the expiration date of your key before that expiry date. If you lose your key, then this date will eventually kick in telling others not to use this key anymore. Enter a **strong passphrase** for the key. This should be one of the complicated passwords you do remember and commit to memory. Your computer login password isn't a bad idea, given that your passphrase will probably be stored in the OS X keychain. You can change this password later.



Click **Generate key**, have fun spamming your mouse or keyboard, and you will have a new PGP key!

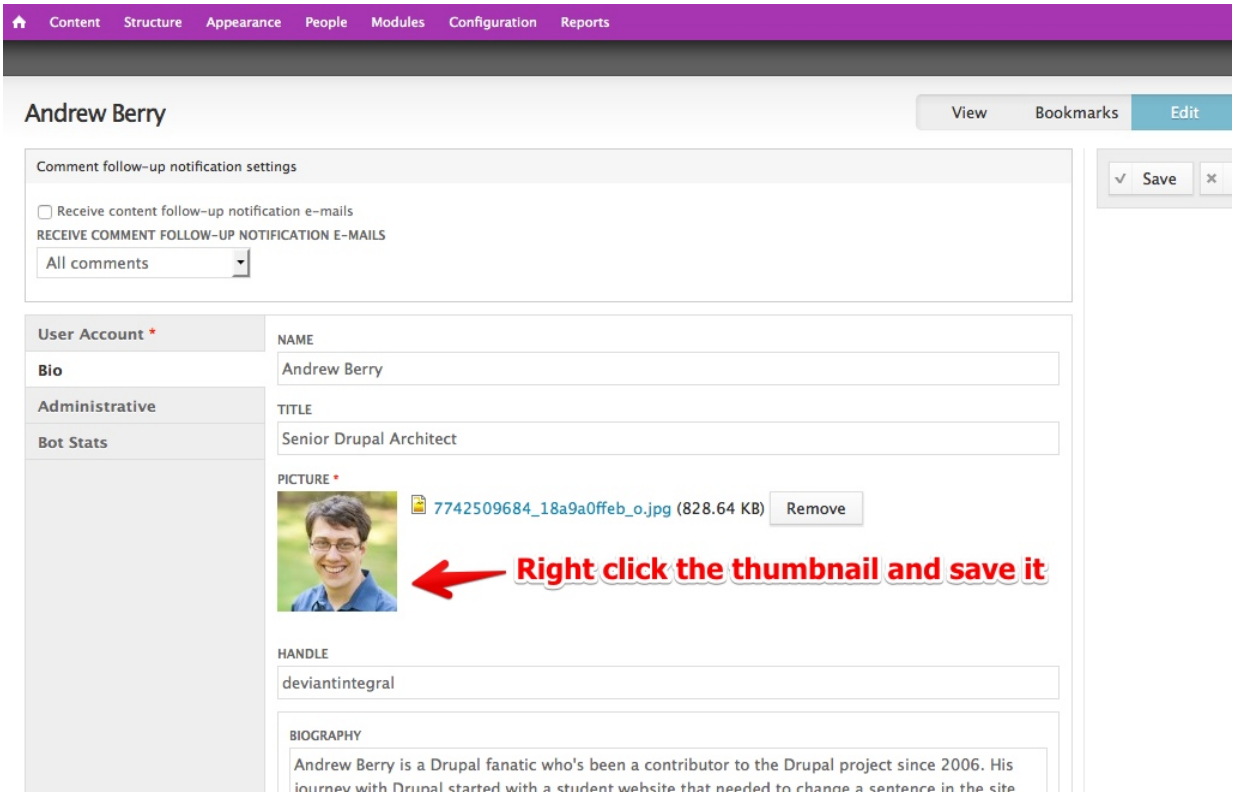
Add additional emails to your key

To add more email addresses to your key, click **Details**, and then **User IDs**. If you have a different legal name from your given name, you can add those in here as well.



Adding your picture to your key

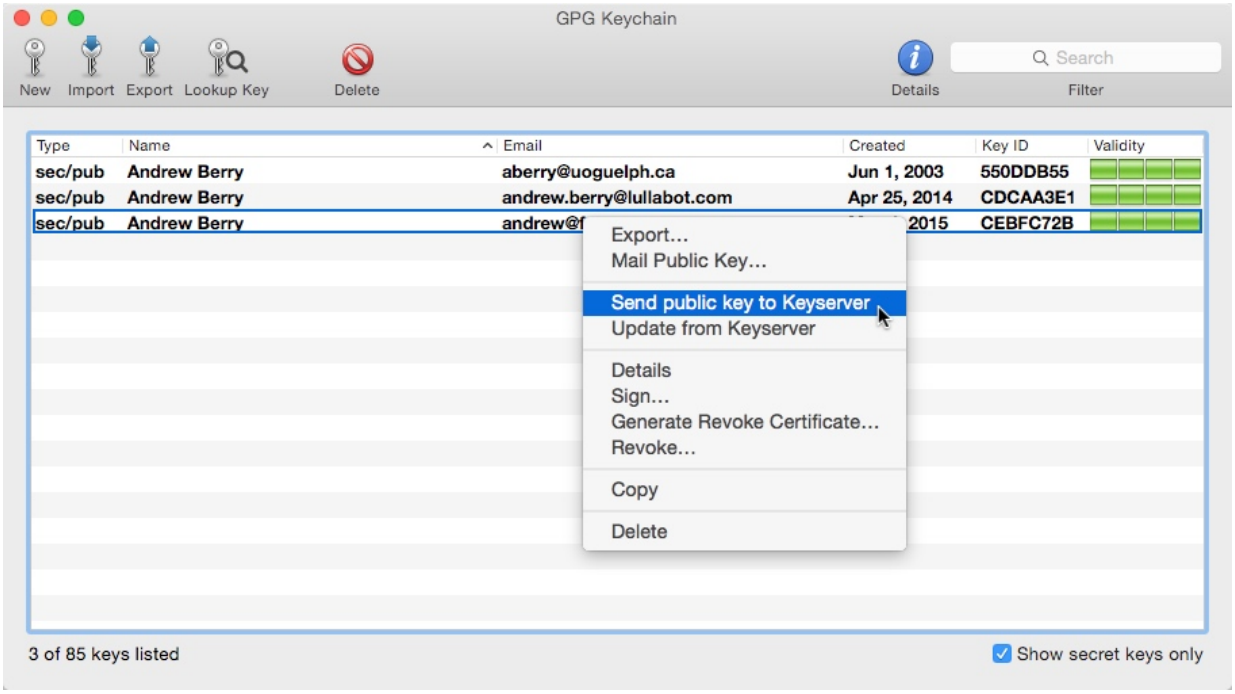
Adding a picture to your key gives yet another way to help validate your identity. PGP keys are shared as small text files, so you don't want to attach a 10MB JPEG to your key. For Lullabot employees and contractors, you can grab a pre-sized thumbnail from your user account edit form on lullabot.com.



Save this file, and then drag it in to the "Photos" tab on your key.

Uploading your public key

Now that your key has been created, upload it to the public key directory. **Any time you update your key's public data, remember to upload it again!**

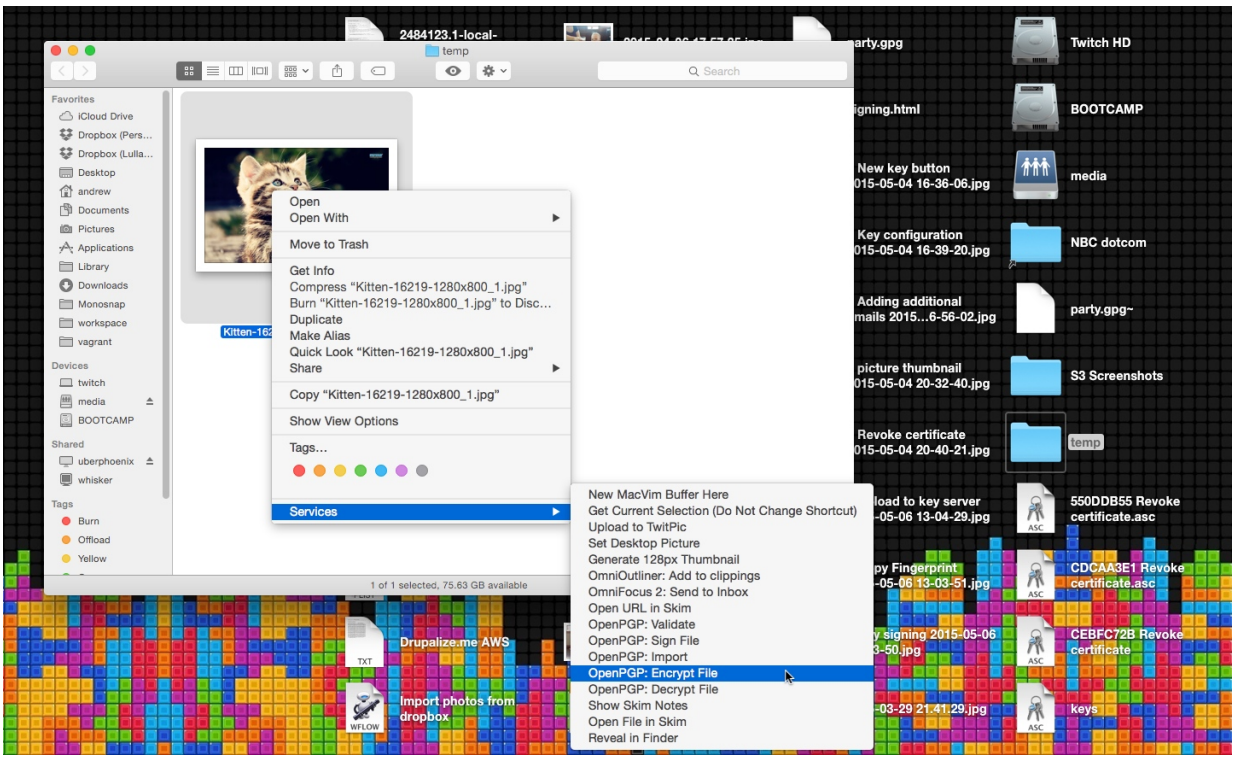


Generating a revocation certificate

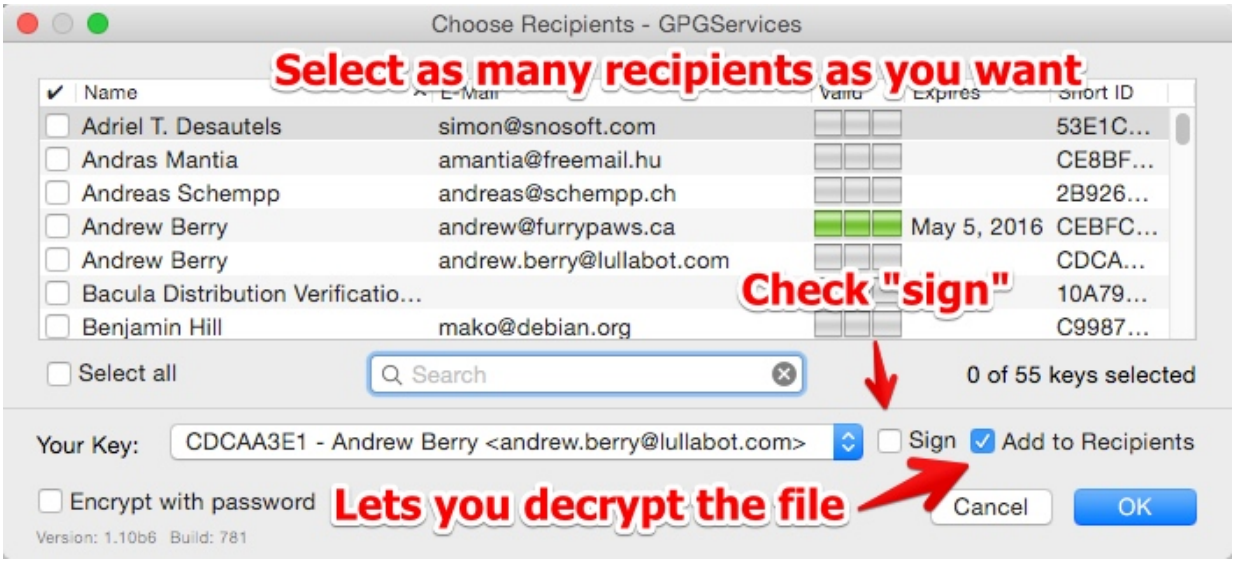
Sometimes you might find yourself in a situation where you've lost control of your key. Perhaps you lost your laptop, or someone you don't trust was using it while you were logged in. A revocation certificate lets you tell the world that a key should no longer be used or trusted. **GPG Tools for OS X** will automatically store a revocation key for you, so as long as your computer is backed up it should always be possible to revoke a lost key.

Encrypting a file

On OS X, right click a file, and "OpenPGP: Encrypt" will show up under the Services menu.



Choose who you want to be able to decrypt the file. In general, you will want to sign the file as well so the recipient knows it was **you** that sent it.



If you chose to sign the file or let yourself decrypt it, you will be asked for your passphrase and a ".gpg" file will be created. This file can be emailed, shared on Dropbox, and so on, and it will be secure. There's a new "Encrypt with password" checkbox as well. That is useful for anyone who hasn't set up a public key yet. **However**, it still leaves you having to communicate that passphrase somehow. **Try to use public keys instead** because they are much easier to use once they are set up.

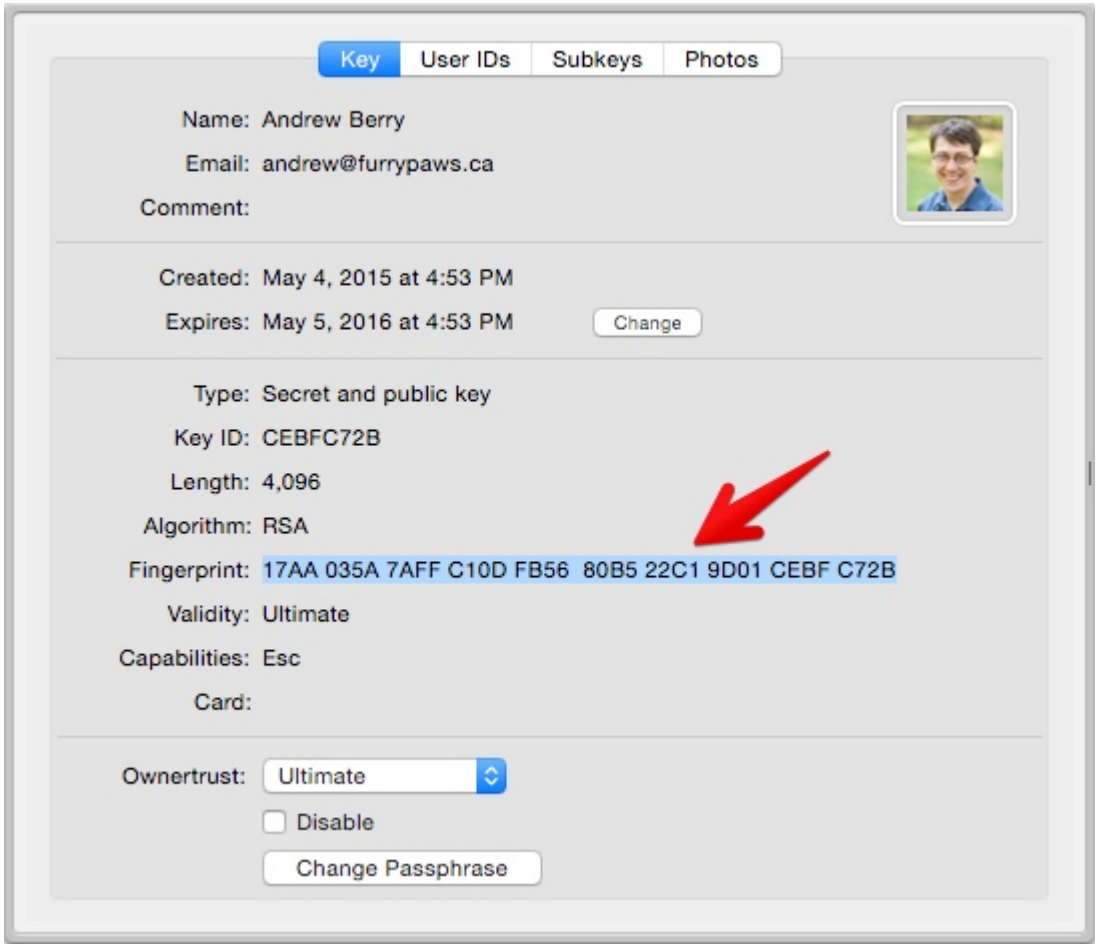
Decrypting a file

Double click the .gpg file, and enter your passphrase. You might not be asked for your passphrase if you recently provided it. If the file was signed, and you have their public key in your keyring, GPG will tell you if it could validate who sent the file as well.

Key Parties and the Web of Trust

If a gaggle of 'bots are getting together in the real world, it's a great chance to sign any new keys! Here's a condensed set of steps taken from The Keysigning Party HOWTO.

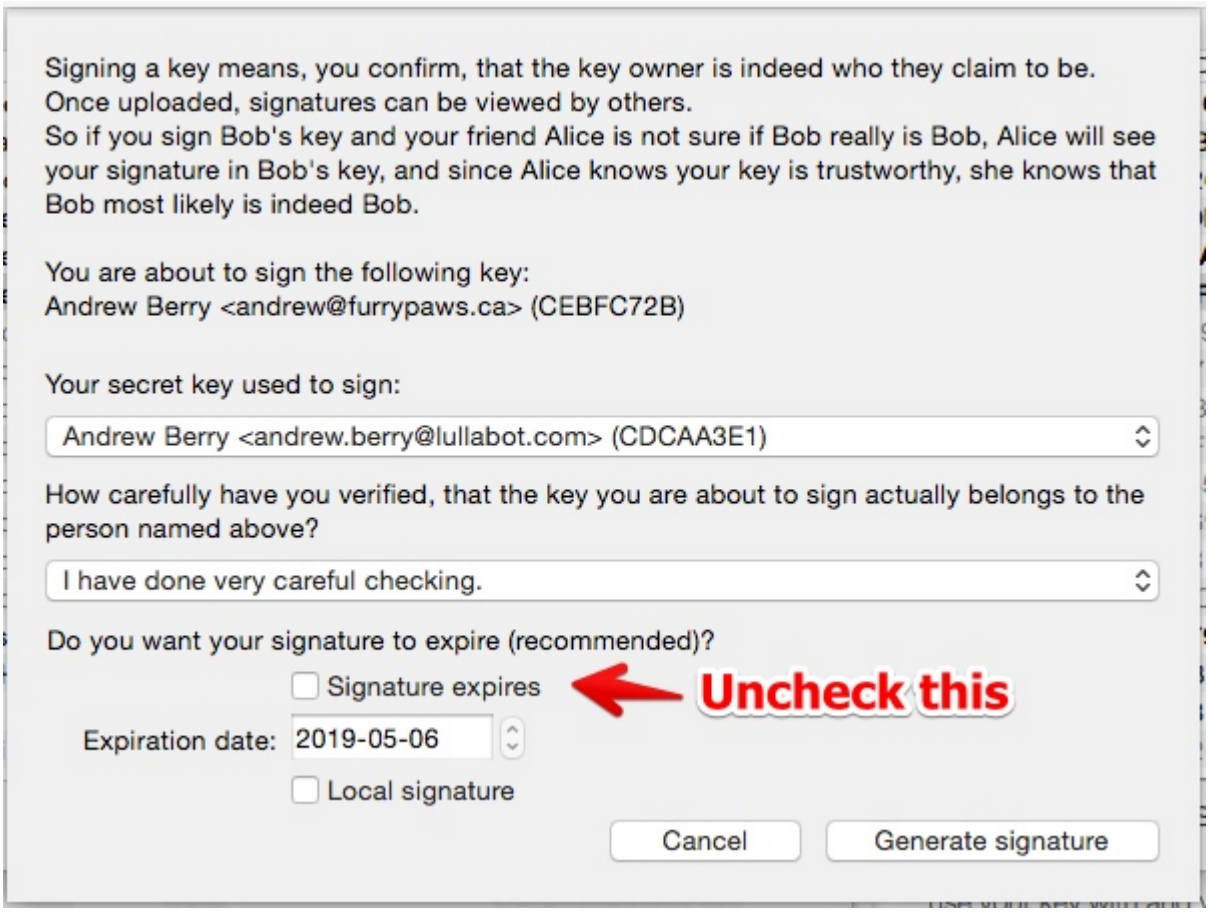
1. Each person should create a key using the above steps.
2. After, they should give the organizer the email attached to the key and the fingerprint of their key.



3. The organizer should import the key from the public server.
   - For the organizer, it's useful to create a separate keyring for the party to simplify creating a key list. `gpg --keyring ~/Desktop/party.gpg --no-default-keyring --recv-keys [KEY-ID]`
4. The organizer should then provide each person with a table of keys they can use to mark the ones they have validated.

Signing a key

Once you have validated a key fingerprint belongs to a person, you can right-click on it and select "Sign". **Uncheck the Signature Expires** checkbox for anyone whose identity you are very confident in. For Lullabot employees and contractors, meeting in person should be enough to select "I have done very careful checking" since HR will have validated identities for employment. For others, check their driver's license or passport. Once the key is signed, upload it to a key server to tell the world about your trust in the identity.



If your key is signed by someone else, you can update your key from the public key servers to add the signature to your local copy of the key.

Validating keys

The algorithm for the "Validity" field is somewhat complex. You might wonder why GPG isn't showing a key you think should be "valid" as valid. To paraphrase the GPG manual:

- Keys you personally sign will show as valid
- At least three "marginally trusted" keys need to sign a key for it to be fully trusted
- The "ownertrust" setting or dropdown on a person's key describes how much you trust that person to validate other keys in your keyring.

GPG tries to be very flexible, and allows you to configure how it determines if keys are trusted or not. For our purposes, we recommend that you leave the GPG settings at their defaults. If your key isn't showing up as valid to others, then the best solution is to get more 'bots to sign your key. If other keys aren't showing up as valid for you, then you should find 'bots who's keys you can sign to bring them in to your Web of Trust.

Appendix

The appendix includes some checklists to help manage security.

Related Links

The items below link to stories on the web that have security ramifications. These stories identify real world hacks and risks that help illustrate the need for security controls.

How Apple and Amazon Security Flaws Led to My Epic Hacking This story describes how the author was targeted by a hacker who got access to his iCloud account. The hacker reset his iCloud, Google, and Twitter passwords, remote-wiped his computer and phone, and then deleted his Google account. Lots of things went wrong in this story, but a couple of things that would have reduced the damage would have been to use strong passwords and 2FA on his Google and Apple accounts, and not to use his Apple email address (one he seldom checked) as the recovery address for his Google account.

Stealing Login Credentials From a Locked PC or Mac Just Got Easier This story describes a way to access login credentials from a laptop computer, even if the computer is locked, by plugging a device into a USB port on the computer. This makes it clear that locking the device is not enough to protect it. The only protection against this threat would be to log out of the computer before locking it.

CEO Mail Fraud: How to Combat a Whale of a Problem This article describes a scam where someone is able to emulate the email address of the CEO or another senior executive, either by hacking their email account or using a look-alike account with a slightly misspelled variation of the corporate domain. The "CEO" then sends an email to someone in the organization asking them to do something, like wire money or pay a bill. The protection against this scam is to use two factor authentication on email requests for money or payment by verifying the request using a second factor, like a phone call to a known phone number.

Device Checklist

Before starting, gather a list of all devices to audit:

- Computers
- Phones
- Tablets
- NAS devices and servers
- Removable media archives
- Any remote / VPS hosted servers you use in your work

With each device, validate:

- [ ] All computers have a complex password with a screen lock timeout.
- [ ] All computer hard drives are encrypted. Include backup Mac Minis, Time Machine backups, and so on. Note that TrueCrypt is no longer considered secure.
- [ ] New Windows computers should have Windows 7 or 8 professional for BitLocker support, or Windows 10. Home editions of Windows should be upgraded.
- [ ] All data that doesn't exist in a cloud service like Dropbox should exist on your computer and an off-site cloud backup. A local backup is really useful for quick restores or Time Machine, but might not be needed if you have a really fast uncapped internet connection.
- [ ] Backups support versioning.
- [ ] At least one backup destination should be "immutable", where existing backups can't be modified. This protects us from CryptoLocker style scams.
- [ ] All backups are encrypted. Cloud services use a private key that only you know.
- [ ] All mobile devices have a PIN and screen timeout set. Only use Trusted Places for automatic unlocks for devices you don't share and at very trusted locations like home. Avoid using Trusted Devices like Bluetooth pairings since it's just as easy to steal a phone and a smartwatch or headset. If your device supports biometrics like TouchID, consider setting a timeout to require a password. iOS doesn't support this for the lock screen, but 1Password does under Settings > Advanced > Security > Require Master Password (1 Hour). If supported, set your device to wipe all data after a certain number of failed unlock attempts. On iOS, this is under "Touch ID & Passcode" in Settings.
- [ ] All remote accounts use 2FA where supported, including Dropbox, Google, Slack, and GitHub.
- [ ] New Android phones like the Nexus 6 should support encryption by default. Due to major performance and compatibility issues with older devices, we omit existing Android devices from required encryption. Check encryption support before buying a new phone.
- [ ] All computer and mobile systems should be patched and up to date.
- [ ] All devices should have "Find" and "Remote Wipe" capabilities.
- [ ] Rooted Android phones and jailbroken iPhones should be treated with care.

After you've finished reading the above, run through these fun scenarios to make sure you're all set!

Backups and Restores

Make sure you'd be safe in the following circumstances:

- [ ] For my primary work computer, I put it in my microwave and cook popcorn on it. Once I purchase a new computer, I restore from a local backup without losing any data. This includes work data stored in my home directory (/Users/myname) that isn't already in the cloud like Dropbox or Google Docs.
- [ ] While myself, my family, and any pets and loved ones are on a wilderness no-technology retreat, a meteor incinerates my house (#rightnow), destroying every computer, phone, tablet, and hard drive I own. After

purchasing new devices, I'm able to regain access to my off-site backups and cloud accounts like Google or Dropbox.

- [ ] At the Lullabot Retreat, I decide to take my laptop fishing. After running into town to replace it, I'm able to restore my data even though I'm not home.

Security and Encryption

Make sure you'd be safe in the following circumstances:

- [ ] I place catnip on my laptop keyboard because I love my cat. My screen lock prevents Kitty from viewing or changing sensitive information.
- [ ] A client puts very important credentials in a Word document I download. I'm not worried about securely erasing the file because my hard drive is encrypted.
- [ ] Sally has asked me to log in to GitHub on her laptop. I'm able to access my password vault using nothing but the internet and things I know in my head. After Sally is done, I manually log out of all accounts I logged in to.
- [ ] I need to move a copy of the Daily Report database at a Lullabot Retreat where the internet is totally broken. I can use my USB drive because I've encrypted the drive using FileVault or BitLocker.
- [ ] I switch from iOS to Windows Phone because it sounds like fun. I'm able to recreate all of my 2FA tokens by using pre-printed recovery codes or SMS messages.

ISO 27001 Cross-Reference

This section provides a cross-reference between the controls required by ISO 27001 and the policies in this handbook that are intended to implement those controls.

5 Information security policies

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

5.1 Management direction for information security

A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.

- Leadership and Review

5.1 Review of the policies for information security

The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

- Leadership and Review

6 Organization of information security

6.1 Internal organization

Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.

6.1.1 Information security roles and responsibilities

All information security responsibilities shall be defined and allocated.

- Leadership and Review

6.1.2 Segregation of duties

Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization’s assets.

6.1.3 Contact with authorities

Appropriate contacts with relevant authorities shall be maintained.

6.1.4 Contact with special interest groups

Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.

6.1.5 Information security in project management

Information security shall be addressed in project management, regardless of the type of the project.

6.2 Mobile devices and teleworking

Objective: To ensure the security of teleworking and use of mobile devices.

6.2.1 Mobile device policy

A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.

- Lullabot VPN
- Passwords and PINs
- Hard Drive Encryption
- Device Lock Screens
- Lost or Stolen Devices

6.2.2 Teleworking

A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.

- Lullabot VPN
- Passwords and PINs
- Hard Drive Encryption
- Device Lock Screens
- Lost or Stolen Devices

7 Human resource security

7.1 Prior to employment

Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

7.1.1 Screening

Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

7.1.2 Terms and conditions of employment

The contractual agreements with employees and contractors shall state their and the organization’s responsibilities for information security.

7.2 During employment

Objective: To ensure that employees and contractors are aware of and fulfill their information security responsibilities.

7.2.1 Management responsibilities

Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.

7.2.2 Information security awareness, education and training

All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.

7.2.3 Disciplinary process

There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.

7.3 Termination and change of employment

Objective: To protect the organization’s interests as part of the process of changing or terminating employment.

7.3.1 Termination or change of employment responsibilities

Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.

8 Asset management

8.1 Responsibility for assets

Objective: To identify organizational assets and define appropriate protection responsibilities.

8.1.1 Inventory of assets

Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.

- Asset Inventory

8.1.2 Ownership of assets

Assets maintained in the inventory shall be owned.

8.1.3 Acceptable use of assets

Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.

- Acceptable Use Policy

8.1.4 Return of assets

All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.

- Asset Inventory

8.2 Information classification

Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.

8.2.1 Classification of information

Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.

8.2.2 Labeling of information

An appropriate set of procedures for information labeling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.

- Asset Inventory

8.2.3 Handling of assets

Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.

8.3 Media handling

Objective: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

8.3.1 Management of removable media

Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.

8.3.2 Disposal of media

Media shall be disposed of securely when no longer required, using formal procedures.

8.3.3 Physical media transfer

Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.

9 Access control

9.1 Business requirements of access control

Objective: To limit access to information and information processing facilities.

9.1.1 Access control policy

An access control policy shall be established, documented and reviewed based on business and information security requirements.

9.1.2 Access to networks and network services

Users shall only be provided with access to the network and network services that they have been specifically authorized to use.

9.2 User access management

Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.

9.2.1 User registration and de-registration

A formal user registration and de-registration process shall be implemented to enable assignment of access rights.

9.2.2 User access provisioning

A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.

- Shared Accounts
- Shared Passwords

9.2.3 Management of privileged access rights

The allocation and use of privileged access rights shall be restricted and controlled.

- Shared Accounts
- Shared Passwords

9.2.4 Management of secret authentication information of users

The allocation of secret authentication information shall be controlled through a formal management process.

9.2.5 Review of user access rights

Asset owners shall review users' access rights at regular intervals.

9.2.6 Removal or adjustment of access rights

The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

9.3 User responsibilities

Objective: To make users accountable for safeguarding their authentication information.

9.3.1 Use of secret authentication information

Users shall be required to follow the organization's practices in the use of secret authentication information.

- Acceptable Use Policy

9.4 System and application access control

Objective: To prevent unauthorized access to systems and applications.

- Acceptable Use Policy

9.4.1 Information access restriction

Access to information and application system functions shall be restricted in accordance with the access control policy.

9.4.2 Secure log-on procedures

Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.

- Acceptable Use Policy

9.4.3 Password management system

Password management systems shall be interactive and shall ensure quality passwords.

- Passwords and PINs
- Password Managers
- Shared Passwords
- Two Factor Authentication

9.4.4 Use of privileged utility programs

The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.

9.4.5 Access control to program source code

Access to program source code shall be restricted.

10 Cryptography

10.1 Cryptographic controls

Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

10.1.1 Policy on the use of cryptographic controls

A policy on the use of cryptographic controls for protection of information shall be developed and implemented.

- Passwords and PINs
- Password Managers
- Hard Drive Encryption
- Backups
- Acceptable Use Policy
- Email Security
- Using PGP/GPG for Secure Communications

10.1.2 Key management

A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole life cycle.

11 Physical and environmental security

11.1 Secure areas

Objective: To prevent unauthorized physical access, damage and interference to the organization’s information and information processing facilities.

11.1.1 Physical security perimeter

Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.

11.1.2 Physical entry controls

Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

- Lullabot VPN
- Passwords and PINs
- Hard Drive Encryption
- Device Lock Screens
- Acceptable Use Policy

11.1.3 Securing offices, rooms and facilities

Physical security for offices, rooms and facilities shall be designed and applied.

11.1.4 Protecting against external and environmental threats

Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.

- Acceptable Use Policy
- Device Maintenance

11.1.5 Working in secure areas

Procedures for working in secure areas shall be designed and applied.

11.1.6 Delivery and loading areas

Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

11.2 Equipment

Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization’s operations.

11.2.1 Equipment siting and protection

Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

- Hard Drive Encryption
- Device Lock Screens
- Acceptable Use Policy
- Device Maintenance
- Malware and Viruses

11.2.2 Supporting utilities

Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.

- Device Maintenance

11.2.3 Cabling security

Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.

- Lullabot VPN
- Malware and Viruses

11.2.4 Equipment maintenance

Equipment shall be correctly maintained to ensure its continued availability and integrity.

- Acceptable Use Policy
- Device Maintenance

11.2.5 Removal of assets

Equipment, information or software shall not be taken off-site without prior authorization.

11.2.6 Security of equipment and assets off-premises

Security shall be applied to off-site assets taking into account the different risks of working outside the organization’s premises.

- Lullabot VPN
- Passwords and PINs
- Two Factor Authentication
- Hard Drive Encryption
- Device Lock Screens
- Lost or Stolen Devices
- Backups
- Acceptable Use Policy
- Device Maintenance

11.2.7 Secure disposal or reuse of equipment

All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

- Hard Drive Encryption

- Device Lock Screens

11.2.8 Unattended user equipment

Users shall ensure that unattended equipment has appropriate protection.

- Hard Drive Encryption
- Device Lock Screens
- Acceptable Use Policy

11.2.9 Clear desk and clear screen policy

A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.

- Acceptable Use Policy

12 Operations security

12.1 Operational procedures and responsibilities

Objective: To ensure correct and secure operations of information processing facilities.

12.1.1 Documented operating procedures

Operating procedures shall be documented and made available to all users who need them.

- Acceptable Use Policy

12.1.2 Change management

Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.

12.1.3 Capacity management

The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.

12.1.4 Separation of development, testing and operational environments

Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.

12.2 Protection from malware

Objective: To ensure that information and information processing facilities are protected against malware.

12.2.1 Controls against malware

Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

- Acceptable Use Policy
- Malware and Viruses

12.3 Backup

Objective: To protect against loss of data.

12.3.1 Information backup

Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.

- Backups

12.4 Logging and monitoring

Objective: To record events and generate evidence.

12.4.1 Event logging

Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.

12.4.2 Protection of log information

Logging facilities and log information shall be protected against tampering and unauthorized access.

12.4.3 Administrator and operator logs

System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.

12.4.4 Clock synchronization

The clocks of all relevant information processing systems within an organization or security domain shall be synchronized to a single reference time source.

12.5 Control of operational software

Objective: To ensure the integrity of operational systems.

12.5.1 Installation of software on operational systems

Procedures shall be implemented to control the installation of software on operational systems.

- Acceptable Use Policy
- Malware and Viruses

12.6 Technical vulnerability management

Objective: To prevent exploitation of technical vulnerabilities.

12.6.1 Management of technical vulnerabilities

Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

12.6.2 Restrictions on software installation

Rules governing the installation of software by users shall be established and implemented.

- Acceptable Use Policy
- Malware and Viruses

12.7 Information systems audit considerations

Objective: To minimize the impact of audit activities on operational systems.

12.7.1 Information systems audit controls

Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes.

13 Communications security

13.1 Network security management

Objective: To ensure the protection of information in networks and its supporting information processing facilities.

- Lullabot VPN

13.1.1 Network controls

Control: Networks shall be managed and controlled to protect information in systems and applications.

- Malware and Viruses

13.1.2 Security of network services

Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.

- Lullabot VPN
- Malware and Viruses

13.1.3 Segregation in networks

Groups of information services, users and information systems shall be segregated on networks.

13.2 Information transfer

Objective: To maintain the security of information transferred within an organization and with any external entity.

13.2.1 Information transfer policies and procedures

Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.

- Acceptable Use Policy
- Email Security
- Security in the Cloud
- Using PGP/GPG for Secure Communications

13.2.2 Agreements on information transfer

Agreements shall address the secure transfer of business information between the organization and external parties.

13.2.3 Electronic messaging

Information involved in electronic messaging shall be appropriately protected.

- Slack Channels
- eMail Groups
- Acceptable Use Policy
- Malware and Viruses
- Email Security
- Using PGP/GPG for Secure Communications

13.2.4 Confidentiality or nondisclosure agreements

Requirements for confidentiality or non-disclosure agreements reflecting the organization’s needs for the protection of information shall be identified, regularly reviewed and documented.

14 System acquisition, development and maintenance

14.1 Security requirements of information systems

Objective: To ensure that information security is an integral part of information systems across the entire life cycle. This also includes the requirements for information systems which provide services over public networks.

14.1.1 Information security requirements analysis and specification

The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.

14.1.2 Securing application services on public networks

Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.

- Lullabot VPN
- Two Factor Authentication
- Acceptable Use Policy
- Email Security

14.1.3 Protecting application services transactions

Information involved in application service transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

- Lullabot VPN
- Passwords and PINs
- Two Factor Authentication
- Acceptable Use Policy

14.2 Security in development and support processes

Objective: To ensure that information security is designed and implemented within the development life cycle of information systems.

14.2.1 Secure development policy

Rules for the development of software and systems shall be established and applied to developments within the organization.

14.2.2 System change control procedures

Changes to systems within the development life cycle shall be controlled by the use of formal change control procedures.

14.2.3 Technical review of applications after operating platform changes

When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

14.2.4 Restrictions on changes to software packages

Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.

14.2.5 Secure system engineering principles

Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.

14.2.6 Secure development environment

Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development life cycle.

14.2.7 Outsourced development

The organization shall supervise and monitor the activity of outsourced system development.

14.2.8 System security testing

Testing of security functionality shall be carried out during development.

14.2.9 System acceptance testing

Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.

14.3 Test data

Objective: To ensure the protection of data used for testing.

14.3.1 Protection of test data

Test data shall be selected carefully, protected and controlled.

15 Supplier relationships

15.1 Information security in supplier relationships

Objective: To ensure protection of the organization’s assets that is accessible by suppliers.

15.1.1 Information security policy for supplier relationships

Information security requirements for mitigating the risks associated with supplier’s access to the organization’s assets shall be agreed with the supplier and documented.

- Security in the Cloud

15.1.2 Addressing security within supplier agreements

All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization’s information.

15.1.3 Information and communication technology supply chain

Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.

15.2 Supplier service delivery management

Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.

15.2.1 Monitoring and review of supplier services

Organizations shall regularly monitor, review and audit supplier service delivery.

15.2.2 Managing changes to supplier services

Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.

16 Information security incident management

16.1 Management of information security incidents and improvements

Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

16.1.2 Reporting information security events

Information security events shall be reported through appropriate management channels as quickly as possible.

16.1.3 Reporting information security weaknesses

Employees and contractors using the organization’s information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.

16.1.4 Assessment of and decision on information security events

Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.

16.1.5 Response to information security incidents

Information security incidents shall be responded to in accordance with the documented procedures.

16.1.6 Learning from information security incidents

Knowledge gained from analyzing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.

16.1.7 Collection of evidence

The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

17 Information security aspects of business continuity management

17.1 Information security continuity

Objective: Information security continuity shall be embedded in the organization’s business continuity management systems.

17.1.1 Planning information security continuity

The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.

17.1.2 Implementing information security continuity

The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.

17.1.3 Verify, review and evaluate information security continuity

The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

17.2 Redundancies

Objective: To ensure availability of information processing facilities.

17.2.1 Availability of information processing facilities

Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.

18 Compliance

18.1 Compliance with legal and contractual requirements

Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

18.1.1 Identification of applicable legislation and contractual requirements

All relevant legislative statutory, regulatory, contractual requirements and the organization’s approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.

18.1.2 Intellectual property rights

Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.

18.1.3 Protection of records

Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislative, regulatory, contractual and business requirements.

18.1.4 Privacy and protection of personally identifiable information

Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.

18.1.5 Regulation of cryptographic controls

Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.

18.2 Information security reviews

Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.

18.2.1 Independent review of information security

The organization’s approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.

18.2.2 Compliance with security policies and standards

Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.

18.2.3 Technical compliance review

Information systems shall be regularly reviewed for compliance with the organization’s information security policies and standards.

Acknowledgement

I understand and agree that I have read and will comply with the policies contained in Lullabot's Information Security Policy.

Name (Printed)

Signature

Date