Flock Safety Internet Security Policy

Overview

The following IT security framework is a collection of existing and new policies and procedures relevant to the IT department's approach to handling security-related concerns. It provides a centralized reference for security policies and provides guidance for communication, monitoring, response, and audit activities related to security. Some policies and systems are in place currently, while others are being undertaken or examined.

1. Definitions

Logical Security – login access to a machine or corporate application
Physical Security – measures pertaining to physical access to corporate technology resources
Security Incident – breach of a security measure; unauthorized access to corporate systems or data from an internal or external source, a malicious attempt to disrupt company resources
Sensitive Data – data with restricted access and/or limited permissions to view or edit
Production Network – any network connected to the corporate backbone, either directly or indirectly, which lacks an intervening firewall device; any network whose impairment would result in direct loss of functionality to Flock Safety employees or impact their ability to do work
Lab Network - any network used for the purposes of testing, demonstrations, training, etc.; any network that is stand-alone or firewalled off from the production network(s) and whose impairment will not cause direct loss to Flock Safety nor affect the production network

2. Process

Flock Safety's IT Security Framework is established to guide the general security concerns and specific measures of the company around its data and technology infrastructure; it will be periodically reviewed and modified as needed. The process for addressing security is made up of the following elements.

Policies & Procedures – Policies and procedures will be established, documented, and maintained in order to safeguard Flock Safety's intellectual property, company assets, and data. These practices will be in keeping with industry standards, and will provide the basis for enforcement and audit.

Monitoring & Response – An IDS will be required and maintained for the Flock Safety Network which is required to send out auto-notifications to appropriate security personal on any severity 1 incidents. AWS networks are accessible only on a need to know basis and is actively monitored via AWS security tools, logs, and audits. Auditing is enabled and unique credentials for each employee will be created where possible. All network logs will be manually reviewed on a period basis.

Security Admin Function – An individual(s) will be assigned responsibility for assisting with design and implementation of security systems and policies, to monitor these systems, and report general status and any issues. The admin will work with the appropriate staff to address any security incidents, and will seek out training and other resources in order to stay abreast of current trends and practices

Reporting & Communication – security metrics will be established, base-lined, and monitored by security admin, with reporting and communication to management; communication will also be coordinated with employees to increase awareness of current and ongoing security concerns including polices, viruses, phishing exploits, etc.

Security Planning & Review – An annual review (ad hoc more frequently as needed) will be conducted of policies, incidents with planning of future security initiatives; also regularly involve Security in general IT planning,

implementations, and change management.

Policies and Procedures

CONFIDENTIALITY OF SENSITIVE INFORMATION

Sensitive information is information, which, if inappropriately disclosed, could cause substantial harm to the company; our customers and vendors, or our employees. This applies to verbal, written and electronic (i.e. e-mailing files) communications. It also includes proprietary and trade secret information. Many of us become familiar with company trade secrets; customer and vendor proprietary information; financial information; and other sensitive information as part of our work responsibility. If you have any doubt whether some information is or is not proprietary, please consult with your manager before taking any action that may compromise the company or other parties.

• Sensitive documents should be locked up, especially after hours, and shredded when no longer needed.
• You should log off/lock your computer/mobile phone before leaving it unattended.
• Mobile devices with access to company resources must have a passcode.
• Encryption should be enabled for all laptops
• Credentials should only be sent via secure channels
• External devices such as portable hard drives or usb drives should not be connected to company laptops.
• Access should be only on a need to know basis. If you do not require access anymore please let manager know to revoke
access as soon as it is not required.
• Lastpass should be used to manage company accounts.
• Customer information stored is limited to only:
• Email
• Name
• Home address (if provided)
• License plate (if provided)
• Credit Card information is strictly **prohibited** from being stored on Flock Safety Servers or Databases

Any employee who has access to credit/background information on customers, employees or vendors is subject to the provisions of the Fair Credit Reporting Act. The Fair Credit Reporting Act provides that any person who knowingly and willfully obtains information on a consumer from a consumer agency under false pretenses shall be fined under Title 18, or imprisoned not more than two years, or both. Also, sharing any confidential information with any person who does not have a legitimate need to know the information is strictly prohibited. An employee who violates this policy is subject to immediate termination. Additionally, any employee found to have obtained information on any person other than a legitimate customer or a potential job candidate as part of the preemployment screening process; will be subject to immediate termination.

All Flock Safety employees and subcontractors will exercise due diligence and best practices to protect sensitive information.

Password Policy

• LastPass is the company supported Password Manager and should be used when possible
• Passwords must be at least 12 characters long
• Passwords must contain numbers, letters, and at lease one special character (!,@,$,#,$,%,^,&,*,etc.)
• Lastpass will be required to be used by all employees
• Passwords should not contain words that are found in a dictionary
• Users will be locked out after 7 consecutive failed login attempts
• Default passwords must be changed

• SAML, 2FA or MFA is preferred when possible and a must for the following:
  • Gmail
  • Dropbox
  • Github
  • Amazon Web Services

File Shares

• Dropbox will be used for shared files secured via username and password.
• Permissions will be set at folder level per user.

Email

• Do not subscribe your Flock Safety email address to non-business related mailing lists. The spam filters we have in place will filter them and you will not receive them. Please use a personal email account for any such mailing lists.

Hosting Environment

The Flock Safety systems are hosted in the cloud, using Amazon Web Services. All hosted production environments will require VPN access and/or multi-factored authentication.

Production environments will be segregated from non-production resources, this includes but not limited to:
• Network
• Application Servers & Services
• Credentials
• VPN Servers
• Databases (Encrypted at rest)

Hosting Environment Maintenance

All systems will be patched as soon as possible. All maintenance will first be performed on a dev environment before promoted to production. Any backups will be encrypted and stored only in approved services/locations.

Logical Access

Logical access to the Hosting environment is gained by accessing the systems using a username, and password over VPN.

Flock Safety Production Support personnel can view logs and configuration data. All internal applications will be password or key protected.

Access to AWS infrastructure is allocated on a role basis roughly divided into 4 distinct roles assigned upon SSO Login.
• Administrator - Full access to all areas of AWS. Limited to only those whose job centers around deployment and management of infrastructure (DevOps)
• Engineering Lead - Elevated configuration access to Storage and Application and Servers
• Engineering - Read access to Storage configurations and limited configuration access to application servers
• S3 - Full access to S3 storage only

Physical Access

All on-site resources will be locked up and only accessible by security personal. All Flock Safety offices will be required to have doors locked and accessible via key fob or HID. All production environments are stored in cloud services and are addressed via hosting providers physical security policies.

Cloud Security

• Physically Hosted in US East Region and will adhere to Amazon's guidelines. (http://aws.amazon.com/compliance/)
• Dropbox guidelines found at: https://www.dropbox.com/business/features#security
• Email – Google Apps will be used to manage email accounts: https://support.google.com/a/answer/60762?hl=en

Protocol

All communication to our application servers is done via HTTPS. An Flock Safety SSL certificate is on all servers including but not limited to development, staging, qa and production. When applicable, a secure connection will be used whenever possible for 3rd party integrations over an unsecured connection.

Handling of 3rd Party Data

All 3rd Party data is required to be handled with the same level of care and security as data generated by Flock Safety.

Telephone Use

Cell phones, pagers and other wireless communication devices for personal use are only to be used during break or lunch periods, and should only be used in the break areas or outside of the building.

Laptops

All laptops will require encryption to be enabled on hard drives. All laptops should auto lock after an idle time of 10 minutes.

Removable Media

Storing company or 3rd party data via removable media should be avoided at all times. If storing information on removable media is required for any reason, it's use should be explicity approved by the Flock Safety Security Team. Data stored on a removable media device must be encrypted at rest and cleaned appropriately once it's need has been satisfied.

Any company or 3rd party data stored on a removable device must stay on premises unless explicity approved by the Flock Safety Security Team.

Never attach or connect removable media (or devices) to company laptops/hardware. A common tactic to gain access to corporate networks, is to leave malware infected media in public areas as "lost". A curious person/employee finds it, plugs it in to see it's contents, and now is infected with a virus, and connected to the private corporate network.

Visitors

Office visitors must be accompianied, or monitored, at all times by an Flock Safety employee. Any suspicious person(s) or activity should be immediately communicated to the Office Manager and/or building security.

Vistors should never have access to any Flock Safety network except the guest wifi. (SSID: FlockSafety-Guest) If access to the private network is needed for any reason, it must be explicitly approved and documented by a member of the Flock

Safety Security team. Documentation should include: date and time, name of visitor, reason for access, device type connected.

ELECTRONIC COMMUNICATION

Electronic communications include telephone, e-mail, internet, intranet, file transfer, electronic forums, faxes and voice mail sent or received by employees with the use of any electronic communications system or service utilized, operated or maintained by or on behalf of Flock Safety. Flock Safety is responsible for securing its network and computer systems in a reasonable and economical manner against unauthorized access and/or abuse, while at the same time making them accessible to authorized and legitimate users. This responsibility includes informing users of expected standards of conduct, and the consequences for not adhering to them. Attempts to violate the provisions of this policy will result in disciplinary action ranging from the temporary revocation of user access to termination of employment. The users of our network and computer systems are responsible for respecting and adhering to local, state, federal and international laws related to the access and use of computer systems and software. Flock Safety will cooperate fully with appropriate authorities to provide information related to actual or suspected activity not consistent with the law. Flock Safety provides internal and external electronic mail (e-mail) facilities to employees for business purposes. You should be aware that whenever you send e-mail, your name, user id, and/or location are included in such e-mail message. Therefore, all e-mail users should exercise good judgment and common sense when creating and distributing e-mail messages. Further, you should be aware that there is no guarantee of privacy with an e-mail message, and that Flock Safety reserves the right to access all aspects of employees' e-mail at anytime for any reason without notice to the employee.

- Forgery (or attempted forgery) of e-mail messages is prohibited.
- Attempts to read, copy, modify, or delete e-mail messages of other users is prohibited.
- Sending harassing, threatening, obscene, inappropriate, or other objectionable messages via e-mail to anyone is prohibited.
- Sending unsolicited junk mail, "for profit" messages, or chain letters is prohibited.
- Passwords for any Flock Safety network system must not be disclosed to any person for any reason.
- You are not authorized to ask any other employee to disclose his/her password to the network or to voicemail.
- Do not leave passwords where others could see them. Treat your password as you would treat cash.
- Passwords may not be transmitted electronically, in print, by voicemail, or through a third party.
- You may not permit any other person to log into or use your password.
- You may not disclose the access codes for restricted areas to any person.
- Downloading files for personal use.

INTERNET ACCESS

As a user of the Company's network and computer system, you may be authorized to access the Internet. You should be aware that every Internet site you visit is capable of determining who you are, and whom you represent, and that Flock Safety tracks this information as well. Accordingly, access to the Internet should include the use of good judgment, common sense, and careful discretion.

- Internet access should be limited to company business only. Visiting game or adult sites and access for personal or other inappropriate use is strictly prohibited.
- Use of Flock Safety's computer systems in attempts to gain unauthorized access to remote systems is prohibited.
- Because of the prevalence of viruses on the Internet, downloading of any programs, data, or other material, except as expressly approved by the Information Technology department, is prohibited. When approved by IT, downloading of programs, data, or other materials must be done on you specific PC's hard drive, and not to the company's network servers.
- Confidentiality of data (including e-mail messages) via the Internet cannot be assured. Accordingly, the transmission of client-sensitive material or other proprietary information, without the express permission of the related client, is prohibited.

Employees encountering any such prohibited use should report it to the network administrator or a Company executive.

Guests such as visiting clients are only permitted to connect to the guest network.

Violations

Any employee found to be abusing the privilege of Flock Safety's access to email or the Internet will be subject to disciplinary action up to and including termination of employment. If necessary, Flock Safety also reserves the right to advise appropriate legal officials of any violations of law.

SOLICITATIONS AND DISTRIBUTIONS

Flock Safety limits solicitation and distribution on its premises because those activities can interfere with the efficient operation of our business. Solicitation and distribution is absolutely prohibited by non-employees. Employees must adhere to the following policy.

The communication systems, of Flock Safety including but not limited to bulletin boards, electronic mail, voice mail, facsimile machines and Company-owned computers are for business use only and may not be used for solicitation and/or distribution purposes. The unauthorized use of the communication systems or distribution or posting of notices, photographs or any other materials on any Flock Safety property is strictly prohibited.

Security Guidelines for Software Development

Introduction

The purpose of this document is to provide best practices and guidelines to development efforts at Flock Safety.

Development Lifecycle

The Flock Safety Lifecycle is based off of Microsoft's Security Development Lifecycle structured around software development life cycle in the following five capability areas:
- Training, policy, and organizational capabilities
- Requirements and design
- Implementation
- Verification
- Release and response

Security Development Lifecycle Applicability

The security development lifecycle will apply to the following:
- Deployed in a business or enterprise environment
- Processes personally identifiable information (PII) or other sensitive information
- Communicates regularly over the Internet or other networks

TRAINING, POLICY, AND ORGANIZATIONAL CAPABILITIES

Employees will be trained on the following:
- Secure design, including the following topics:
- Attack surface reduction
- Defense in depth
- Principle of least privilege
- Secure defaults
- Secure coding, including the following topics:

• Cross-site scripting
• SQL injection
• Weak cryptography
• Security testing, including the following topics:
• Differences between security testing and functional testing
• Risk assessment
• Security testing methods
• Privacy, including the following topics:
• Types of privacy-sensitive data
• Privacy design best practices
• Privacy development best practices
• Privacy testing best practices

REQUIREMENTS

The requirement phase should address security concerns to mitigate issues later in development. This includes but not limited to:
• Quality Service Level Agreements (SLAs) set?
• Bug SLAs set?
• Will authorization and authentication be required?
• Determine will a stand-alone security design reviews be required?
• Does penetration testing need to be performed?
• Does fuzz testing need to be performed?
• What is privacy impact rating?
• High - The feature/product deals with PII
• Moderate - May impact privacy
• Low - No impact to privacy

DESIGN

The design phase should include but not limited to:
• Are attack surfaces covered?
• What firewalls are required?
• Is feature restricting or disabling access to system services?'
• Is proper cryptography services being used where applicable?
• Are security principles being applied?
• e.g. Principle of least privilege

IMPLEMENTATION

The implementation phase should include but not limited to:
• Latest versions of Enterprise standard web framework technologies are being leveraged (e.g. Grails, Spring & Spring Security)
• Security warnings addressed by compilers
• Unsafe functions are not being used
• Static analysis tools run
• Code has been reviewed by at least 2 developers with focus on:
• Following internal coding standards for clarity, naming and design
• Security & Performance Implications
• Meets intended requirements
• Automated checks for the existence of tests run
• Code under review is programatically blocked from merging into the code base if the any check fail
• When a Code Review is merged tests automatically performed in our development environment

• Development databases are sanitized to prevent the use and leakage of production data

VERIFICATION

The implementation phase should include but not limited to:
• Are user privileges working as expected?
• Fuzz testing needed?
• Review attack surfaces again? Preferably by external team that developed it.

RELEASE AND RESPONSE

The release & response phase should include but not limited to:
• A incident response plan is created with the following defined:
• Emergency contacts
• Security service plan
• May have a list of security activities that were performed
• Data related Quality & Bug SLAs performance
• May have versions of technologies used

Miscellaneous Security Requirements

PENETRATION TESTING

Penetration testing will be performed on an annual basis. PCI pen testing template will be used to test external facing applications and services. AWS Security tools and tests will also be performed for internal white box testing.

SECURITY BLOGS/NEWSLETTERS

The security team will be registered and notified via email or other form of notification (Twitter, website) on known security risks and vulnerabilities. These will be addressed based on threat level.

ACCESS

• 2 Factor Authentication is required on all company logins that support 2 factor (Email, GitHub, etc)
• 2FA messages are directed to security personal for any high-level administrative account
• Access limited to need to know basis

APPLICATIONS & NETWORK

All applications and networks must meet the following requirements, any deviations from these requirements must be approved by the security team:
• Secure authorization
• Abuse lockout
• Role based permissions where applicable
• Anomaly detection and alerts on application server logs
• Automatic sanitization of inputs
• ORM database layer to prevent attacks via SQL Injection
• Communication between application services and tools is done through SSL/TLS encrypted connections (internal network included)
• Non-production and production networks are segmented to limit the security implications in the event of a breach
• Firewalls are in place with limited ports accessible
• Guest network should be used for non-Flock Safety personal
• Usage of both log level and passive network anomaly detection implemented

DATABASE

- Field level encryption on sensitive fields such as PINS and passwords
- Production DB files are file level encrypted
- Production DB has Failover redundancy
- Daily backups

Data Breach Response Policy

PURPOSE

The purpose of the policy is to establish the goals and the vision for the breach response process. This policy will clearly define to whom it applies and under what circumstances, and it will include the definition of a breach, sta roles and responsibilities, standards and metrics (e.g., to enable prioritization of the incidents), as well as reporting, remediation, and feedback mechanisms. The policy shall be well publicized and made easily available to all personnel whose duties involve data privacy and security protection.

Flock Safety's Information Security's intentions for publishing a Data Breach Response Policy are to focus significant attention on data security and data security breaches and how Flock Safety's established culture of openness, trust and integrity should respond to such activity. Flock Safety Information Security is committed to protecting Flock Safety's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

BACKGROUND

This policy mandates that any individual who suspects that a theft, breach or exposure of Flock Safety Protected data or Flock Safety Sensitive data has occurred must immediately provide a description of what occurred via email null@flocksafety.com or immediately contact a member of Flock Safety's security team (Dev Ops, I.T., V.P. Engineering or CTO).

The e-mail address is monitored by the Flock Safety's Information Security Administrator. The security team will investigate all reported thefts, data breaches and exposures to confirm if a theft, breach or exposure has occurred. If a theft, breach or exposure has occurred, the Information Security Administrator will follow the appropriate procedure in place.

SCOPE

This policy applies to all whom collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifiable information or Protected Health Information (PHI) of Flock Safety members. Any agreements with vendors will contain language similar that protects the fund.

CONFIRMED DATA BREACH

As soon as a theft, data breach or exposure containing Flock Safety Protected data or Flock Safety Sensitive data is identified, the process of removing all access to that resource will begin.

The Information Security Administrator will chair an incident response team to handle the breach or exposure.

The team may include members from:
- Upper Management
- Engineering/Dev Ops
- Information Technology
- Operations (if user data is affected)

• Human Resources
• The affected unit or department that uses the involved system or output or whose data may have been breached or exposed
• Additional departments based on the data type involved, Additional individuals as deemed necessary by the Information Security Administrator

The Information Security Administrator will be notified of the theft, breach or exposure. I.T., along with the designated forensic team, will analyze the breach or exposure to determine the root cause.

WORK WITH FORENSIC INVESTIGATORS

As provided by Flock Safety cyber insurance, the insurer will need to provide access to forensic investigators and experts that will determine how the breach or exposure occurred; the types of data involved; the number of internal/external individuals and/or organizations impacted; and analyze the breach or exposure to determine the root cause.

DEVELOP A COMMUNICATION PLAN

Work with Flock Safety communications, legal and human resource departments to decide how to communicate the breach to: a) internal employees, b) the public, and c) those directly affected.

Ownership and Responsibilities

ROLES & RESPONSIBILITIES:

• **Sponsors** are those members of the Flock Safety community that have primary responsibility for maintaining any particular information resource. Sponsors may be designated by any Flock Safety Executive in connection with their administrative responsibilities, or by the actual sponsorship, collection, development, or storage of information.

• **Information Security Administrator** is that member of the Flock Safety community, designated by the Chief Technology Officer, who provides administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources in consultation with the relevant Sponsors.

• **Users** include virtually all members of the Flock Safety community to the extent they have authorized access to information resources, and may include staff, trustees, contractors, consultants, interns, temporary employees and volunteers.

• The **Incident Response Team** shall be chaired by the Information Security Administrator and shall include, but will notbe limited to, the following departments or their representatives: Information Technology, Engineering, Communications, Legal, Management, Financial Services, Operations, and Human Resources.

Enforcement

Any Flock Safety personnel found in violation of this policy may be subject to disciplinary action, up to and including termination of employment. Any third party partner company found in violation may have their network connection terminated.

Definitions

• **Encryption or encrypted data** – The most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text;

• **Plain text** – Unencrypted data.

• **Hacker** – A slang term for a computer enthusiast, i.e., a person who enjoys learning programming languages and computer systems and can often be considered an expert on the subject(s).

• **Protected Health Information** (PHI) - Under US law is any information about health status, provision of health care, or payment for health care that is created or collected by a "Covered Entity" (or a Business Associate of a Covered Entity), and can be linked to a specific individual.

• **Personally Identifiable Information** (PII) - Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered

• **Protected data** - See PII and PHI

• **Information Resource** - The data and information assets of an organization, department or unit.

• **Safeguards** - Countermeasures, controls put in place to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. Safeguards help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset.

• **Sensitive data** - Data that is encrypted or in plain text and contains PII or PHI data. See PII and PHI above.

Clean Desk Policy

PURPOSE

The purpose for this policy is to establish the minimum requirements for maintaining a "clean desk" – where sensitive/critical information about our employees, our intellectual property, our 3rd parties could be left unprotected. It's important that sensitive information is protected from accidental exposure or loss.

SCOPE

This policy applies to all Flock Safety employees and affiliates.

POLICY

1. Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
2. Computer workstations must be locked when workspace is unoccupied.
3. Computer workstations must be retained by the assigned party after working hours, no device shall be left on premises unattended for extended periods of time.
4. Whiteboards containing Restricted and/or Sensitive information should be erased.
5. Any Restricted or Sensitive information must be removed from the desk and locked in a drawer or locker when the desk is unoccupied and at the end of the work day.
6. File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
7. Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.
8. Passwords, api keys, and other sensitive data should never be sent/stored in plain text - including written down in any accessible location.
9. Printouts containing Restricted or Sensitive information should be immediately removed from the printer.
10. Restricted and/or Sensitive documents should be disposed of in a secure manner when no longer needed.

11. Portable computing devices such as laptops and tablets should remain in the custody of the party it was assigned.
12. All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

POLICY COMPLIANCE

Compliance Measurement
The Flock Safety Security Team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, business tool reports, internal and external audits, and feedback to the policy owner. At a minimal, the Flock Safety Security team will complete an internal audit on an annual basis.

Exceptions
Any exception to the policy must be approved by the Security team in advance.

Non-Compliance
An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

List of Third Parties of Concern

This document is intended to idenfity all third parties that Flock Safety either utilizes or conducts business with. Along with the entities named below, the level of information that they have (eg. deal with PII or do not deal with PII) is enumerated with the corresponding header. This document is meant to be a living document of all third parties and will be maintaned as third party relationships change.

PARTIES THAT STORE CUSTOMER PII

Below is a list of third parties that store PII for any amount of time. Most services only store PII for a temporary period of time for analysis or reporting purposes.

Services that are hosted by the following parties have granular privileges for Flock Safety employee access and are protected by our Identity Management Solution.
- Amazon Web Services (AWS)
- Dropbox
- Slack
- Chartio
- Segment
- FullStory
- Google Analytics
- LogDNA

PARTIES THAT DO NOT STORE NOR ANALYZE CUSTOMER PII

The following section regards parties that do not store nor analyze customer PII in any stage of information transmission or the software development process.

Identity and Access Management
- Google

Product Management
- Github
- Trello
- Airtable

Infrastructure
- Heroku
- DynDNS
- EasyDNS
- JFrog
- Name.com
- Webflow
- New Relic

Security, Monitoring, and Compliance
- Backbone Security
- Qualsys
- DigiCert
- Klipfolio
- Chartio
- Cisco Meraki
- Pingdom

DEVELOPER TOOLING & SOFTWARE

The following is a list of tooling and software that Flock Safety Employees use in accordance with the Acceptable Use Policy. Although none of the tooling below inheriently stores or analyzes PII, employees may on a case-by-case basis expose the following systems with PII data.

Please note that although the list below is as comprehensive as possible, third party software, libraries, plugins, and other non-major dependencies to the software below are not covered in the scope of this document. For any additional information, please contact the Flock Safety Security Team.

Operating Systems (OS) in Use
- Apple OS X
- Amazon Linux
- Ubuntu

Web Browsers in Use
- Chrome
- Safari

Security & Encryption
- OpenVPN
- Keka

Integrated Developer Environments (IDEs)
- IntelliJ
- Sublime
- Atom

Other Tooling/Software
- Adobe Systems
- Microsoft Office
- Postman
- Homebrew

- Docker
- Quip

Updates to This Document

Flock Safety's Information Security Administrator will update this document on an annual basis and inform employees of key changes. If you have any questions or see the need for updates within this doc, please contact null@flocksafety.com