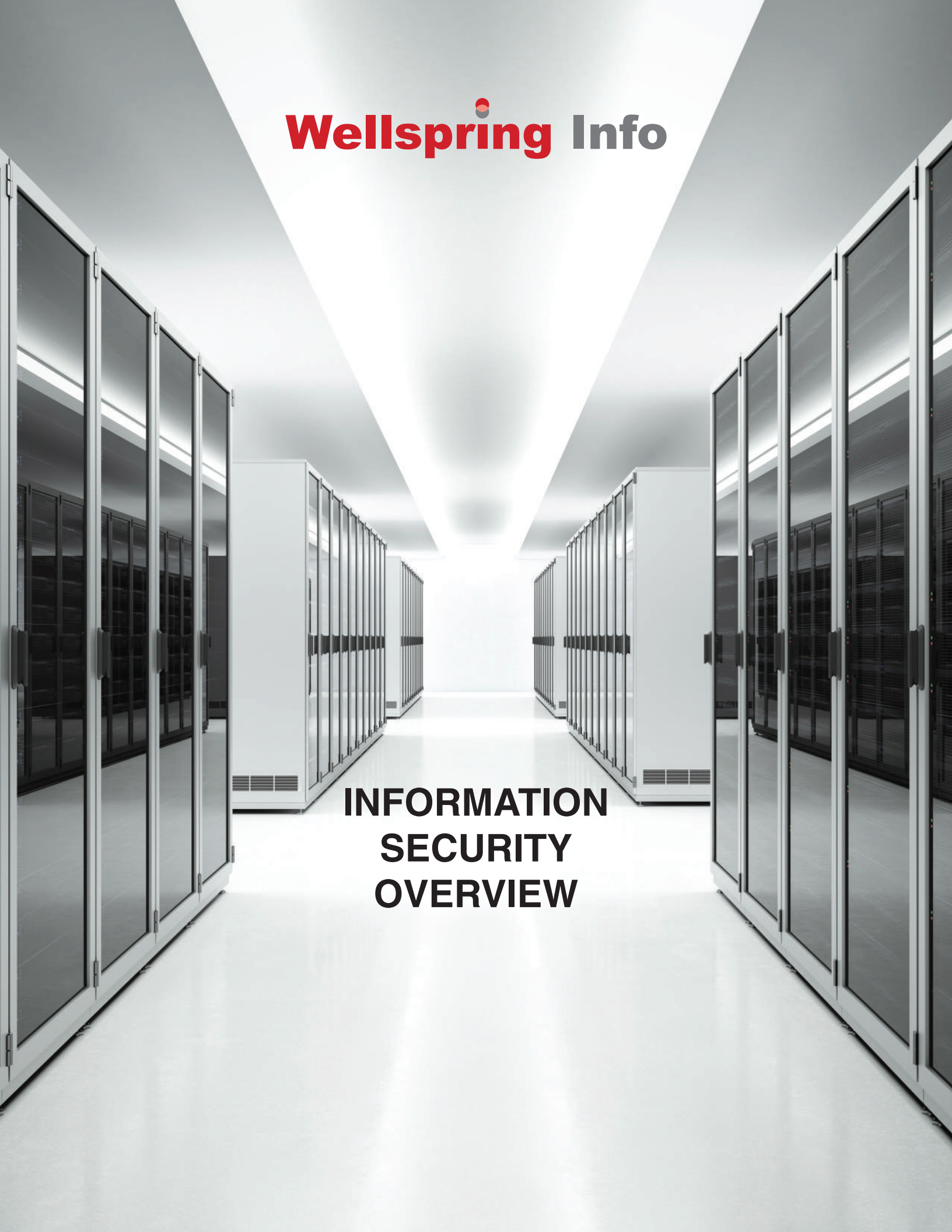

Wellspring Info

INFORMATION SECURITY OVERVIEW

Introduction

Wellspring Info's security framework is based on the comprehensive set of security requirements and controls outlined in our Information Security Plan. We take a complete and holistic approach to information security, and as such, we're continually updating and improving our Information Security Plan.

Our main information security strategic objectives are:

1) Data loss prevention: Reduce the likelihood of data loss / disclosure of confidential or federally protected data.
2) Improve security of systems and networks.
3) Proactive risk management.
4) Crisis and security management: Initiatives that will help us recover our information assets in the event of a data breach.

Information Security Plan

The purpose of our Information Security Plan is to mitigate risks by establishing proper controls and security standards. This plan is a living, breathing document that is continually reassessed, audited, improved, and trained upon, to ensure cross-functional information security.

Managing Information Assets

We have created an inventory of document hardware, applications (both internal and third party), databases, and other information assets, and assigned each with a custodian who is responsible for its ongoing security.

Off-Site Storage

As outlined in our Disaster Recovery Plan, which is part of our Business Continuity Plan, we maintain off-site storage of all critical legal, insurance, and financial documents, along with our recovery plans, to enhance our ability to fully function at all times.

Protecting Sensitive Information

Wellspring Info has multiple safeguards in place to protect sensitive data and network equipment, including technical controls that safeguard our computer hardware, software, and access controls (management and operational controls such as security policies, operational procedures, personnel, physical security & environmental security).

Risk Mitigation

We employ the following metrics to measure and prioritize our risks: Likelihood of occurrence and impact of occurrence. Each risk has a mitigation strategy in place; each mitigation strategy is monitored, updated and improved.

Emergency Action Plan

As award-winning emergency response experts who have read and improved thousands of emergency response plans, including the city of Philadelphia's emergency response plan for the Pope's visit, we have a robust, high-level Emergency Action Plan which utilizes leading procedures from the Department of Homeland Security, FEMA, the FCC, NOAA, USPS, the New York Police Department, American Red Cross, OSHA, the CDC, the Department of Labor, the FBI, and other industry leaders.

Third-Party Vendor Assessments

We conduct assessments to ensure that our vendors are compliant with our information security requirements. Questions we like to ask include:

1) Do you review security at each phase of the software development lifecycle?
2) What methodologies do you use for security testing your products?
3) Do third parties conduct security assessments on your products?
4) Do you have security squads that attack your products prior to release?
5) Do you use automated tools for security testing or code review?

Cloud provider certifications:

- Google Cloud Security: https://cloud.google.com/security/
- Google Cloud Privacy & Compliance: https://cloud.google.com/security/compliance
- Atlassian Cloud security: https://www.atlassian.com/trust/policies/cloud-security
- Atlassian Cloud compliance: https://www.atlassian.com/trust/compliance

Media Sanitation Policy

We do not back-up on zip drives, disks, or other easily-stolen media.

Audits

Internal audits are used to ensure that:

- Our policies and procedures in place are effective.
- Controls are being properly implemented.
- Risk is being managed.
- Our information security plan continues to be updated, improved and implemented.
- Our training is ongoing and effective.

Redundancy

Our apps are backed up on the Google cloud, one of the largest cloud providers in the world. Our secure content management system (where the content is held prior to its being converted to an app) is provided by Atlassian, a software and cloud company serving 85 of the Fortune 100. We keep local copies of both the content and the app which we could use at another service provider, if necessary. Both Google and Atlassian are widely considered industry leaders in security and reliability.

Other information security highlights include:

- Routers are updated with software patches.
- Network equipment is kept physically secure.
- Security alarms are on premises.
- We perform application security testing.
- Rules for the configuration, maintenance, and use of our network infrastructure.
- All internal network traffic that carries or potentially carries sensitive information is encrypted and integrity protected.
- We do not operate a VPN which would allow remote access to our network.
- Operating system hardening is applied uniformly across the server system.
- A process exists for installing updates and security patches for operating systems.
- Backups are tested.
- Outbound email infrastructure use Opportunistic TLS to request remote servers upgrade to an encrypted connection.
- We run new versions of Chrome OS, macOS, and browsers.
- We do not use Internet Explorer.
- Service accounts are restricted to system-use only and are not leveraged by users for access.
- Our content management team uses Chromebooks which features multiple layers of security including built-in virus protection, verified boot to block viruses & malware, and automatic updates of latest versions.
- We use strong passwords for privileged accounts (minimum of 9 characters with at least 4 character types). Passwords are changed annually.

If you have any questions, please let us know: Security@WellspringInfo.com