Security is Priority Number One

KNOWiNK has taken a unique and leading role in ensuring electronic poll book (EPB) security.

The Poll Pad and ePulse systems maintain multiple levels of security to ensure confidentiality and integrity of all devices, communications, data, and systems. To verify our system is secure, we have security policies, certifications, and third party audits available to the Jurisdiction upon request.

Hardened to U.S. Federal Security Benchmarks

KNOWiNK has hardened our systems to Department of Homeland Security Cyber Infrastructure Security Agency (DHS CISA) benchmarks for both the AWS account and the operating systems used by the application server instances. Hardened where feasible to Level 1 of the CIS Foundation Benchmarks for AWS these requirements increase the security of the AWS system used by KNOWiNK. These requirements set forth stringent application controls which increase the security of the AWS system used by KNOWiNK. More information can be found here:

https://d0.awsstatic.com/whitepapers/compliance/AWS_CIS_Foundations_Benchmark.pdf

Homeland Security Praises KNOWiNK Poll Pad/ePulse Security

In 2020—well ahead of the November elections—we began working closely with the Department of Homeland Security, Cyber Infrastructure Security Agency (DHS CISA) to perform a penetration test of the KNOWiNK Poll Pad and ePulse System.

The examiners performed an in-depth test of the application including testing for OWASP Top 10 vulnerabilities, NIST 800-53, and the NIST Cybersecurity Framework. The report showed an overall strong security posture with an examiner describing it as a “well configured application with a limited attack vector.” No critical or high vulnerabilities were found and only one medium and one low finding were found and corrected immediately. Moreover, our Poll Pad and ePulse application code has been reviewed line-by-line by U.S. states from coast to coast. In addition to (DHS CISA, Elections Canada, Idaho National Laboratory, and Centers for Information Security have all performed penetration tests on our systems.

In addition to our efforts with DHS. KNOWiNK has taken an active role with CISA, participating in their processes and maintaining direct contact communication regarding our process, escalation, and research. We are also fully aligned with the FBI Cyber Security team, with whom, as necessary, we communicate directly.

Independently Active in Enhancing Election Security

KNOWiNK participates fully in the CISA-RABET-V project, in which we engage with other Election Software companies in developing a fully integrated code/process review RABET-V for verifying the security election technology.

We are also currently working with noted security consultants on updating our information in:

- Risk Register
- Data Classification
- Cyber Incident Checklist
- Penetration Test process

Dedicated Hardware Resources for Increased Security and Reliability

Moreover, the KNOWiNK solution is implemented as a single tenant solution for some jurisdictions but is an option to all. Using this model, instead of hardware resources being shared among multiple customers, each customer is hosted on their own dedicated server. This setup increases both security—separate servers protect customer data from breaches by limiting a breach to only the data on the breached server so no other customer's data (stored on their own dedicated servers) is compromised—as well as reliability, as the separate and dedicated processing resources preclude one customer's increased processing demand from affecting any other customer's processing capability.

Multiple Cloud Defenses, Plus Encryption

Built on the industry-leading Amazon Web Services (AWS) Cloud, the ePulse system uses multiple defenses to keep the system both secure and available during peak periods. In 2018, and for the eighth year in a row, Gartner, a leading technology scoring and research company, has named AWS as the best provider in the industry. Some of the encryption features KNOWiNK has deployed to protect the data housed in Poll Pad and ePulse include:

- Encrypted Traffic–All traffic to and from ePulse and between Poll Pad and ePulse is encrypted using TLS 1.2 encryption, a certificate authority signed certificate, and AES 128 or 256 bit encryption, depending on what the user's browser supports. All traffic is encrypted using an AWS managed service, ensuring it is always up to date with the latest encryption standards and supported by industry leading AWS network teams.
- Amazon Aurora Database–The Aurora Database is a managed database service that provides the highest level of performance, availability, and security. All data contained in the ePulse system is stored in the Amazon Aurora Database. The data is encrypted at rest and in transit with an encryption key stored in the secure Key Management Service (KMS). In addition, full backups are performed on a nightly basis and stored for 30 days in multiple data centers. Point-in-time backups are also available for a minute-by-minute backup. During peak election periods, failover databases are used in multiple availability zones to prevent any database or network outage. The failover process completes in seconds if an outage were to occur.
- Amazon S3 Storage–Amazon Simple Storage Service (S3) is used to store all data that cannot be stored in a database, such as signature images, file backups, generated reports, etc. S3 is a highly reliable and secure storage service that features 99.999999999% file durability and 99.99% availability. In addition, all files stored in S3 are encrypted at rest and in transit and their access is governed by IAM (identity and access management) policies which only allow resources that need access to have it.

Secure Operating System

The Ubuntu operating system used by the application servers are also built upon a server image provided by CIS that is hardened to level 1 v1.0.0 of the Ubuntu 16.04 operating system benchmarks. These ensure the operating system is not left open to any security vulnerabilities. More information on these benchmarks is available at: **https://learn.cisecurity.org/benchmarks**

Apple iPad Security

As the leader in mobile technology security, the Apple iPad has been certified to FIPS 140-2 by NIST for the cryptographic algorithms that protect data stored on the unit. The iOS operating supports VPN technology, remote erase/ wipe, and automatic lock/password requirements. For security purposes, iPads do not have a USB port or allow users to connect any external hardware.

The Poll Pad system only transfers data over 256-bit encrypted Secure Sockets Layer (SSL) connections to and from the remote server. Within the cloud infrastructure, the database uses 256-bit Advanced Encryption Standards (AES) for at-rest encryption to store all information. The database is located on a server that is not publicly accessible and does not have a connection to the internet. For more information about the security of the iOS operating system, please see: https://www.apple.com/business/docs/iOS_Security_Guide.pdf

Secure from Unauthorized Use and Data Access and Restricted Access to External Media

The Poll Pad and ePulse are secure from unauthorized access. The virtual private cloud (VPC) and numerous security systems secure Poll Pads and ePulse from unauthorized access. The Poll Pad operates in guided access mode, which prevents the user from exiting the application, and further, the Poll Pad requires either one or two poll workers to login using login credentials that can be customized by the Jurisdiction.

Encryption Type and Levels

All data stored in both Poll Pad and ePulse is encrypted in transit and at rest.

Poll Pad uses built-in iOS encryption to encrypt the application and all data contained within. Certified by the National Institute of Science and Technology (NIST) to Federal Information Processing Standards (FIPS) 140-2, the iOS operating system uses the most secure encryption standards available to keep data confidential. All communications will be encrypted and isolated on private networks.

- Encrypted Traffic – All traffic to and from ePulse and between Poll Pad and ePulse is encrypted using TLS 1.2 encryption, a certificate authority signed certificate, and AES 128 or 256-bit encryption, depending on what the user's browser supports. All traffic is encrypted using an AWS managed service, ensuring it is always up to date with the latest encryption standards and supported by industry leading AWS network teams.
- Amazon Key Management Service - Used to store all encryption keys that are used to encrypt all data within AWS GovCloud. KMS is a secure method to store encryption keys that not only prevent Amazon from accessing them but also require authorization by any service to access any keys stored within KMS.

Data transferred between Poll Pad and ePulse is encrypted using industry leading TLS 1.2 encryption and uses a signed certificate to stop man-in-the-middle attacks.

All data stored in ePulse is encrypted at rest and during transit within the system. All databases use AWS-powered encryption with encryption keys stored in the AWS key management service.

Audit Logs

Poll Pad has a real-time audit log integrated into the application. The audit log tracks and timestamps every user event that is performed in the application and has the ability to filter down information by general, user, and error events. The user may also print the logs to a thermal or full-sized printer. Timestamps and signatures are collected for each transaction on the Poll Pad and may be audited in ePulse.

Audit logs are exported in near real time from the devices to ePulse and are stored in perpetuity in the AWS GovCloud S3 and Aurora Databases for perpetuity. ePulse uses AWS Cloudwatch to provide a detailed audit trail of user interactions and backend processes. Using AWS Shield, all traffic passes through Amazon's Shield product, which provides both detection and mitigation of distributed denial of service (DDoS) attacks.

Audit logs may also be exported to an iSync drive in exported format then decrypted later into a plain text based file.

Hardened Defenses

KNOWiNK works with our customers to ensure only pre-approved devices are connected to the Poll Pad's network.

Secure Wireless Connection

Only devices which are enrolled in KNOWiNK's licensed Meraki system and have the proper credentials which are loaded during initial provisioning using a QR code generated by ePulse are allowed to connect to ePulse. MAC address filtering on each hotspot is an option that can be configured to prevent any non-approved devices from connecting to the hotspot. For example, Solano County sets up a unique SSID for each jetpack / Poll Pad combo by precinct.

Additionally, iSync drives and Poll Pads require an official apple signed certificate for the Poll Pads and the iSync drives to interact. Any Apple device without this signature built in will not have access.

Server Operation Systems

The Poll Pad and ePulse are secure from unauthorized access. All server access is controlled via the IAM system from AWS which allows only users authorized by the administrator to connect to and manipulate the operating system. The virtual private cloud (VPC) and numerous security systems secure the Poll Pads and ePulse from unauthorized access.

Security and Patching

The Poll Pad system uses the iOS mobile operating system, the most secure mobile operating system on the market. iOS is built only to run on Apple hardware, making it much easier to build a complete, hardened security ecosystem of hardware and software. iPad is Federal Information Processing Standards (FIPS) 140-2 compliant and is the leading choice for government agencies for secure hardware solutions. iOS typically provides several years of Operating System (OS) support on hardware releases - longer than any other mobile OS. Crucial security updates may be deployed past the major OS release lifecycle as minor updates. KNOWiNK maintains certification with the latest versions of the OS as required by the State.

Additionally, as KNOWiNK adds new capabilities to the solution, we apply for an expedited, incremental certification to ensure the Poll Pad solution is always approved for use.

On average, updates to the iPad's iOS and Poll Pad application are done twice a year. Updates will always be scheduled by KNOWiNK and typically occur at least a month before an election. Updates to the ePulse server are thoroughly tested before major releases. If a known vulnerability is issued for any software, a security patch release can be made within 48 hours. In the event of a data breach, we will follow the processes described in our Information Security Policy, which is available upon request.

Staff Login Management

Poll Pad can restrict access through a series of logins that are centrally managed in ePulse. Basic functions are optionally controlled by a base poll worker authentication. More advanced functions can be enabled by entering a supervisor or override password. Authentication is customizable and can include one or two-person authentication with ability to increase complexity of password requirements.

System Can Be Used with a Private Mobile Connection System Over a WAN/MPLS

The Poll Pad solution supports a broad range of connectivity options which include cellular LTE connections. Cellular connections can be leveraged using the built-in cellular networking capacity of the iPad hardware, or by deploying LTE-enabled hotspots to provide connectivity through a traditional wireless connection to multiple devices at once.

As a Verizon partner, KNOWiNK can route all traffic via an MPLS upon request. If the jurisdiction uses their own provider, KNOWiNK can work with the provider to connect to the MPLS.

Secure Data Exchange

All data stored in both Poll Pad and ePulse is encrypted in transit and at rest. All data transmissions occur using encrypted HTTPS connections with a California signed certificate. No data is transferred within or outside of the system without encryption. Communication between devices at the Vote Center and between the Vote Center and ePulse is handled via a secure wireless connection. Communication between the Vote Center and ePulse is 256-bit AES encrypted and meets State requirements.

Poll Pad uses built-in iOS encryption to encrypt the application and all data contained within. Certified by the NIST to FIPS 140-2, the iOS operating system uses the most secure encryption standards available to keep data confidential.

Data transferred between Poll Pad and ePulse is encrypted using industry leading TLS 1.2 encryption and uses a signed certificate to stop man-in-the-middle attacks. All databases use AWS-powered encryption with encryption keys stored in the AWS key management service.

Meraki Mobile Device Management Suite for Remote Management and Security

For swift response and recovery, KNOWiNK uses the Meraki Mobile Device Management (MDM) suite to manage its devices, and has the ability to geolocate, disable, wipe, and lock any Poll Pad or component containing sensitive or confidential voter information if removed from an authorized location, accessed by an unauthorized user, or used for an unauthorized purpose. Meraki's MDM is cloud based and requires no internal servers to operate. All Poll Pads are pre-enrolled in the Meraki MDM prior to shipment to the County and this service is provided to the County at no charge. The licensed Meraki MDM provides the County and KNOWiNK comprehensive management, security and deployment of its Poll Pads. Meraki MDM has capabilities to manage all aspects of the iPad—from wallpaper to powering the iPad off. With profile configuration management, considerable changes may be made to the iPad with little impact in the iPad behavior.

MDM Security Features

- Bluetooth and Wi-Fi are both locked down
- Clear passcodes
- Lock devices
- Selective wipe
- GPS location
- Lost mode
- Passcode policy configuration
- iOS Single App Mode (Kiosk) configuration

MDM Managed Features

- Keep device names up-to-date
- Automatically trust enterprise apps
- Black list unused apps
- Remote iOS updates
- Power control of device.
- Push back iOS updates
- Device process list
- Allow removal of system apps – This allows the removal of any apps not used.

All KNOWiNK iPads are shipped enrolled in a mobile device management (MDM) system powered by Cisco Meraki. The MDM system allows for tracking, remote wipe, and Apple's lost mode which allows the iPad to be locked down remotely until it is returned. Furthermore, with Apple's Device Enrollment Program, an iPad is locked to an MDM server, even after resetting or wiping the device. KNOWiNK uses the MDM to configure the devices according to the Centers for Information Security (CIS) benchmarks for iOS devices where possible.

Virus Invincibility

In a recent study conducted by McAfee, a premier electronic security company, 97% of mobile viruses were created for the Android operating system. A large anti-virus company recently asked Apple to open their operating system to allow anti-virus software to be created for iOS. Apple declined because there is no need for anti-virus software due to the locked down nature of the operating system.

Secure, Yet Familiar and Easy to Use

The Poll Pad application has been built to run exclusively on the Apple iPad tablet. With its ease-of-use and the widespread familiarity of Apple iOS, Election Workers generally know right from the start how to use the iPad, making training on the Poll Pad application easier while keeping Election Workers focused on the election-oriented elements and not the technology. Additionally, the iPad and its IOS platform deliver the most secure tablet available on the market: Apple has ensured that the device meets Federal Information Processing Standards (FIPS) and National Institute of Standards and Technology (NIST) standards, so it does not require any additional appendages or insecure add-on memory cards to operate.