MESSAGE FROM THE FOUNTAIN COUNTY CLERK

Citizens of Fountain County,

Since the vote center concept became a reality in Indiana elections in 2007, leaders in Fountain County have been carefully observing its effect on voters, county budgets, and on the election process.

The following pages layout our plan to make vote centers a reality in Fountain County. The vote center concept gives any voter in Fountain County the opportunity to cast their ballot at any vote center location throughout the county. No one is restricted to one polling place on Election Day. In addition to making it easier for voters on Election Day, the vote center concept also calls for increased early voting opportunities at what are called "satellite vote centers" that are open prior to Election Day.

The most common question we hear in elections is "Where is my polling place?" or "Why can't I just vote at the polling place across from where I work or drop off the kids for school?" A common complaint we hear is "I can't make it back to the polls by 6:00 p.m. on Election Day." Vote centers address these common voter concerns.

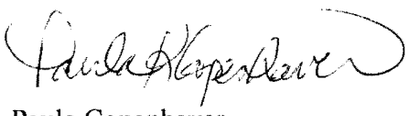
Another important part of the vote center concept is the financial impact it will have on Fountain County. Having to staff fewer locations and provide less equipment to support on Election Day will help the county to realize a cost savings on items such as rental costs, poll worker costs, and equipment costs.

By moving to vote centers, voter's convenience is improved; election administration is streamlined and made simpler; and this improves the county's long-term fiscal stance when it comes to elections.

Most Americans have been voting under the same process for over 50 years. Vote centers represent a major step forward and bring elections into the 21st Century.

I want to thank all the wonderful people who have worked so hard and in a bipartisan manner to move the county toward vote centers. Fountain County should be proud of its community leaders who work together for what will be best for all citizens. To all the churches, community centers, schools, and businesses that have willingly allowed us to use their facilities as vote centers, we are forever grateful.

Warmest regards,



Paula Copenhaver
Fountain County Circuit Court Clerk

FOUNTAIN COUNTY VOTE CENTER PLAN

In Compliance with IC 3-11-18-1-4, the Fountain County Election Board proposes to adopt a plan for the establishment of Voting Centers in Fountain County, to provide more convenient, efficient, cost effective voting access, and procedures for all Fountain County voters. We would like to have this plan go into effect for the 2018 Primary Election.

Fountain County plans to utilize 5 vote center locations. Indiana Code 3-11-18.1-6 only requires one vote center per 10,000 active voters, but the Fountain County Election Board plans to provide one vote center per roughly 2,094 active voters

As of November, 2017:

(A) Total number of registered voters within Fountain County – 11,051
(B) Total number of active voters within Fountain County – 10,469
(C) Total number of inactive voters in Fountain County – 582

1. The following are suggested vote center locations to be open on Election Day:
(The following locations will be reviewed and amended prior to each election cycle)
   A. Attica High School – 211 E Sycamore St., Attica, IN 47918
   B. Covington High School – 601 Market Street, Covington, IN 47932
   C. Veedersburg Fire Station – Community Room – 100 S Main St., Veedersburg, IN 47987
   D. Hillsboro Church of the Nazarene – 453 S SR 341, Hillsboro, IN 47949
   E. Kingman American Legion – 251 W State St., Kingman, IN 47952

2. The following is the suggested satellite vote center location to be open for Early Voting the two Saturdays prior to the election:
   (The following location will be reviewed and may be amended prior to each election cycle)
   A. Fountain County Clerk's Office, 301 4th Street, Covington, IN 47932
   All vote center locations meet the accessibility requirements under IC 3-11-8.

3. Each Vote Center will have one Inspector, two Judges, and four Clerks. At least one Judge will be from the opposite party as the Inspector. Training procedures for poll workers will remain the same. The number of workers, electronic poll books, and voting machines sent to each location will be determined and may be changed by the County Clerk at his/her discretion.

4. Every Ballot type for each precinct, applicable school board elections and party in primary elections shall be available, electronically, at each Vote Center.

5. Fountain County will continue to use the AccuVote TSX touch screen machines. Because the AccuVote TSX is Direct Recording Electronic (DRE) touch screen machine, the requirement in Indiana Code 3-11-18.1-14 that requires ballots to be kept separately by precinct is easily met. Just as in traditional elections, at the end of Election Day, votes will still be tallied and reported by precinct. The voting machines are at no point ever hooked up to the internet. Attached is the TSX diagram.

6. An Electronic Poll Book will be used in order for voters to go to any location that they choose to vote. Fountain County has decided to utilize KNOWiNK innovative election solutions. This electronic poll book will be securely connected to every vote center and to the County Election Board at the Fountain County Clerk's Office on Election Day. It will securely connect every satellite vote center and meets all standards set out by Indiana law under IC 3-11-8-10.3. In addition, KNOWiNK election managers have intimate knowledge and experience with electronic poll books. A minimum of two electronic poll books will be available at each Voting Center.

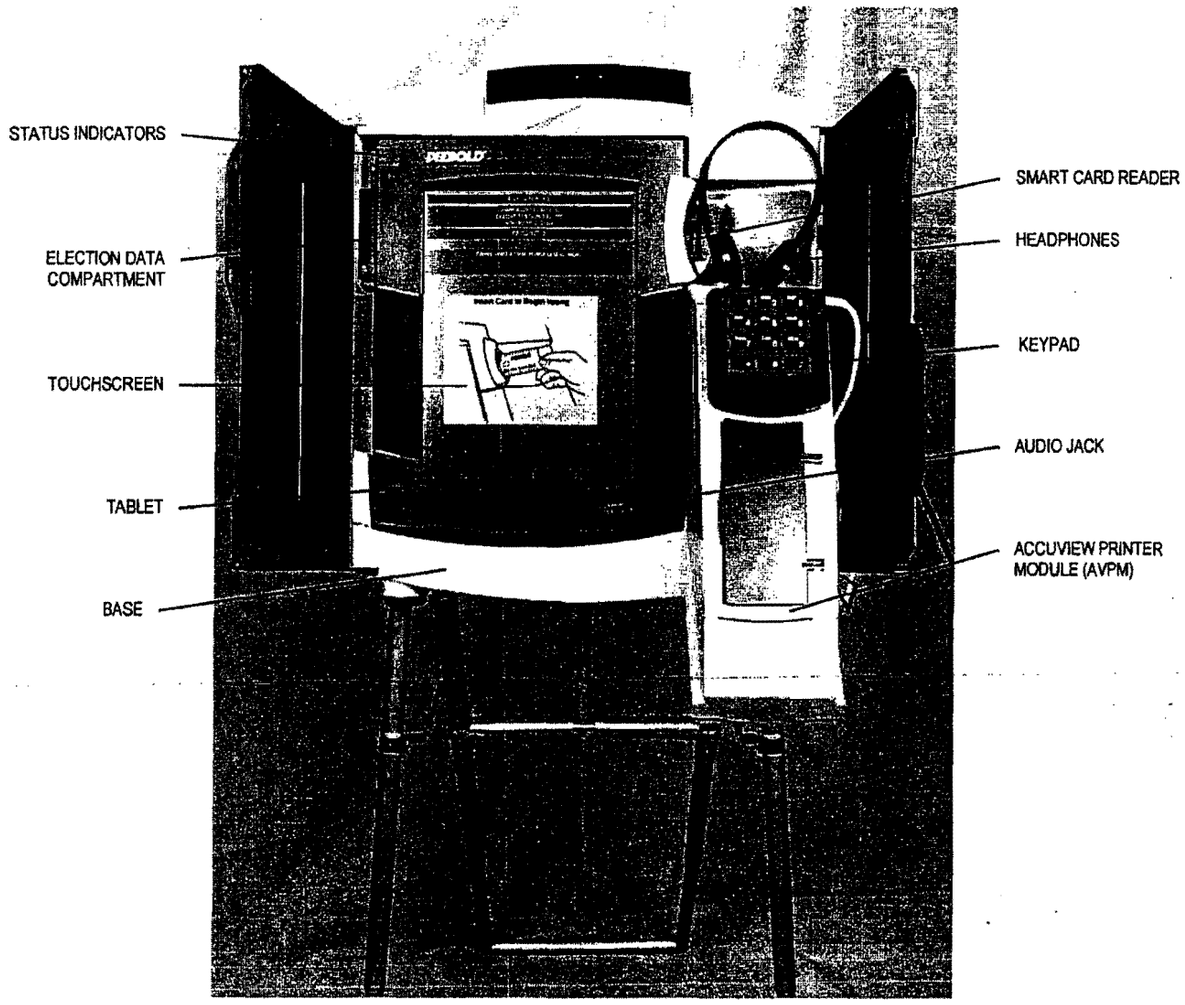
NOTE: Voters from every precinct may vote at any vote center location or satellite vote center location. Every ballot style for each precinct in Fountain County will be available at each vote center and each satellite vote center (Depending on the election, the number of ballot styles varies greatly; therefore, this plan does not attempt to provide a specific number of ballot styles). Each vote center and early vote center will be connected to all other vote centers or early vote centers (as well as the County Election Board) via electronic poll books connected via secured internet lines. At least two electronic poll book terminals will be available at each location.

7. Electronic Poll Book Description and Security Details: The hardware, software and firmware used for the poll pad, will be utilizing the KnowInk Poll Pad. The Poll Pad e-poll book application software runs on the Apple iPad tablet. This system is certified by the Indiana Secretary of State's Office. The Poll Pad system interfaces with Quest Voter Registration System as part of the certified system. See attached for detailed information.
   The number of voters on the machines and the number of voters in the poll pad will be checked and balanced each day.
   In the event of a power failure at each or one vote center, the voting machines and poll pad will be switched to battery backup. For obvious reasons, if the safety of voters and or poll workers is ever at risk, the Fountain County Security Plan will go into effect with instructions from the Fountain County Clerk, Fountain County Election Board, Fountain County EMA, and the Fountain County Sheriff.

8. Fountain County has a full media and community outreach strategy that will involve press releases to newspapers and radio stations. In addition we will use our county web site www.fountaincounty.net to prepare Fountain County citizens for this change. Moreover each voter will receive a postcard in the mail prior to the initial elections, informing them of this change and where each vote center is located. The Clerk and/or her staff will also be available to attend community events and speak about the change.

TSX

AccuVote TSX Component Diagram



GBS
GOVERNMENTAL
BUSINESS SYSTEMS

OVERVIEW

Elections must be fair, accurate, auditable, and secure. AT KNOWiNK, we uphold this responsibility: Poll Pad solution performs without fail - election after election - securely and accurately providing access to the ballot box.

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 system supports VPN technology, Remote Erase/Wipe, and Automatic Lock/password requirements. For security purposes, iPads do not have a USB drive or allow user to connect any unauthorized external hardware. iPads are configured in such a manner (guided access mode) that will not allow a poll worker the ability to even exit the application without a password. In addition, the Poll Pad system only transfers data over 256 bit encrypted SSL connections to and from the remote server. Within the cloud infrastructure, the database uses 256 bit AES at rest encryption to store all information and 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

KNOWiNK Poll Pad utilizes Amazon GovCloud which meets stringent IT certifications. For more information, visit this website for certification standards:

http://aws.amazon.com/govcloud-us/security/

sales@knowink.com · 855.765.6723 · www.knowink.com · 2111 Olive Street, St. Louis, MO 63103

SECURE DATA

All data stored on Poll Pad is encrypted using the iOS operating system that has been validated to FIPS 140-2 by NIST.

All data transferred to and from Poll Pad is encrypted using 256 Bit SSL encryption.

User access, password changes, and all other actions are logged for each specific user and are available to administrators at any time.

All user actions are logged and available for audit if suspicious behavior is detected. In addition, users are required to respond to CAPTCHA challenges if any password cracking is detected while logging into a user's account.

- The system is designed from the ground up with security in mind. All Poll Pads use the iOS operating system which can be secured with a password to prevent any breach in sensitive voter information. All data is also encrypted in transit and at rest.

- KNOWiNK utilizes Mobile Device Management (MDM) to deploy all Poll Pads. By using the MDM, iOS devices can be programmed to lock down access on the device. Users can be denied access to install or uninstall applications or download any malicious software that could compromise the device. In addition, when enrolled, if lost or stolen, MDM has the capability to track, locate, and remotely wipe a device.

sales@knowink.com · 855.765.6723 · www.knowink.com · 2111 Olive Street, St. Louis, MO 63103

POLL PAD HARDWARE

Utilizing DOD and Military-Approved Technology - The Pentagon and Department of Defense have approved iOS for use in military and classified operations. The Department of Justice and NSA consider the encryption utilized within iOS to be virtually impenetrable. Along with a customized version of Android by Samsung and Blackberry, iOS is the only mobile operating system approved for use by the DOD.

Locking Down the iOS Device - Fortunately, the Apple iPad was designed from the ground up to be easy to use for everyone, from children with autism to seniors who may have a difficult time reading text on the screen. In fact, in a 2012 study by eMarketer, iPad growth in the 65+ age group is expected to be one of the fastest growing age groups of iPad users. Seniors are turning to iPads because they are easy to use, whether they have technical skills or not.

Apple iOS devices can be programmed to lock the device down. Users can be denied access to install or uninstall applications or download malicious software that could compromise the device. In fact, while using Guided Access Mode, the device can be locked to a single application. With Guided Access Mode enabled, it would be impossible for a user to exit the application, even after restarting the device, without entering a pass code. All Poll Pads are shipped with tight device restrictions, so you can be assured your Poll Pad will not be vulnerable to outside applications that could compromise the device.

Guided Access (Kiosk) Mode - Built into the iOS operating system, helps people with autism or other special needs stay focused on the task (or application) at hand. Guided Access limits an iOS device to stay on one application by disabling the Home and Power button. With Guided Access mode enabled, your poll workers will never be able to leave the application or even turn off the device. Never worry about a poll worker mistakenly exiting the application or changing any settings. These are just some of the features built into the iPad to make it accessible for everyone. To learn more about iPad accessibility, go online to: http://www.apple.com/accessibility/ios/

Application Sandbox - Apple has built iOS on a solid foundation that is security minded from the ground up. All applications are held in a "sandbox," a separate environment for each application. Each application has a separate file system that cannot be accessed from any other application. Apple has designed iOS so one application cannot infect

sales@knowink.com · 855.765.6723 · www.knowink.com · 2111 Olive Street, St. Louis, MO 63103

or collect information from another.

Virus Invincibility - In a recent study conducted by McAfee, an electronic security company, 97% of mobile viruses were created for the Android operating system. In fact, 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.

Security Features of Poll Pad Bluetooth Sync - Bluetooth 4.0 Security Standards - All iOS devices support Bluetooth 4.0, the latest standard in Bluetooth communication. Bluetooth 4.0 is the most secure Bluetooth standard available employing multiple security features to safeguard voter data.

Please refer to NIST documentation "Guide to Bluetooth Security" (Special Publication 800-121 Revision 1) for more information on Bluetooth 4.0 Security. Poll Pad follows the recommended security implantations in Section 4.4 of the guide.

Mobile Device Management (MDM) - All iPads are shipped enrolled in a mobile device management server powered by Cisco. The mobile device management server allows for tracking, remote wipe, and Apple's lost mode which allows the iPad to be locked down until it is returned. Furthermore, with Apple's Device Enrollment program, an iPad is locked to a mobile device management server, even after resetting or wiping the device. Lost or stolen

The iOS operating system excels and allowing administrative control of the operating system. All Poll Pads are sent pre-enrolled in a mobile device management system, allowing administrators to lock or control nearly every aspect of the system. The app store, game center, news app, entertainment apps, etc. are all locked out from use and able to be controlled by the MDM. A poll worker can be restricted to never leave the Poll Pad application using Guided Access mode, a feature which locks down the device to a single application.

FREQUENTLY ASKED QUESTIONS

How are access control methods, password protection and login access levels such as kiosk or Election mode managed?

All iOS applications are sandboxed, preventing any application or user from accessing that application's data. In addition, by using guided access mode, the election authority can prevent any system settings changes without the use of a passcode.

What security measures are available to protect the operating system, application programs and data on all System equipment from unauthorized change?

iOS has been certified by NIST to FIPS 140-2 and encrypts all data and data transmission on the device. All data is encrypted both at rest and in transit, preventing any outside entity from deciphering or spoofing fraudulent data.

What encryption and other security measures are in place to protect data if the proposed system involves Internet or Cloud based transmission of data to and from EPB components?

iOS, being a feature limited operating system, only allows code that has been code signed by Apple to run on the system. Meaning no unauthorized applications or "viruses" could be loaded onto the system that could cause suspicious behavior.

Will the Poll Pad detect and prevent any suspicious software behavior any part of the System?

Built on the iOS operating system, Poll Pad operates in a fully sandboxed application container. This prevents other applications or outside access to its data or engage in any suspicious behavior that affects Poll Pad. Data stored in Poll Pad is encrypted by the operating system and locked behind a passcode.

ePulse prevents suspicious behavior in several layers. The first layer prevents any outside actor from accessing the system via the application firewall. Only ports 80 and 443 are accessible and only the load balancers are open to public access. Using alerts

provided to system administrators via AWS Cloudwatch, suspicious behavior can be stopped or mitigated as soon as it happens.

All devices are enrolled into an MDM (Mobile Device Management) server. The MDM has the capability to remotely locate, lock, or wipe a stolen or lost device.

How are Poll Pads tracked, recovered, or disabled if stolen or removed from the polling location?

iOS only allows authorized hardware to connect to an iPad that has been digitally signed by Apple. Our iSync drive has been certified by Apple only to contain and transfer approved files. No off the shelf or unauthorized USB devices can connect to an iPad or our application.

DATA TRANSFER PROTOCOLS

Poll Pad uses a simple transfer process within ePulse. The voter data file is exported from the jurisdiction's Voter Registration System to a .csv or .txt based text file. The file is uploaded via a file loader in ePulse and converted to a proprietary, secure, object oriented data base file for use within ePulse and with the iPad's data base.

For Poll Pad Data Import, the data transfer/download request is initiated from the Poll Pad's Tools & Settings section of the device Menu list. Voter database files are then loaded to iPads via an encrypted Wi-Fi connection or a flash drive.

During Election Day, check-ins and signatures are captured and stored on each Poll Pad in an encrypted database. If connectivity is allowed during the Election Day data is automatically background synced with ePulse.

After the election, the data is manually transferred from each Poll Pad back to ePulse via the Voter History Upload option within the Poll Pad's Tools & Settings section of the device Menu list.

Following the confirmation that all data has successfully uploaded to ePulse, the jurisdiction will be able to create an import file that will batch import voter history into the jurisdiction's Voter Registration system. The jurisdiction will also have the ability to generate an electronic roster file listing all voters, their captured signatures, and other data.

All data transferred to and from the Poll Pad is encrypted with 256-bit AES encryption.

sales@knowink.com · 855.765.6723 · www.knowink.com · 2111 Olive Street, St. Louis, MO 63103

NETWORK SECURITY

The Poll Pad and ePulse systems maintain multiple levels of security to ensure confidentiality and integrity of all devices, communications, data, and systems. We have security controls incorporated to safeguard the confidentiality and integrity of data passing over public networks, and to protect the connected solutions.

Within the cloud network of ePulse, the data base server is stored on a non-public accessible server behind a firewall. In addition, KNOWiNK utilizes the VPC (Virtual Public Cloud) security features offered by Amazon GovCloud to isolate network traffic in Central Command from public access. All externally accessible servers are limited to ports 80 and 443 for http and https connections. All users are immediately redirected to a secure connection for the duration of their session when using ePulse.

KNOWiNK will work with the county to create a secure WiFi network that will be used exclusively for Poll Pad. This network only needs external internet access and can be completely separate from any internal network utilized.

Built on the industry leading Amazon Web Services GovCloud, the ePulse system utilizes many defenses to keep the system both secure and available during a peak period such as an election. For the 6th year in a row in 2016, Gartner, a leading technology scoring and research company, has named Amazon Web Services as the best provider in the industry. KNOWiNK utilizes many of the security and scalability features built into Amazon Web Services, meaning ePulse is secured with the best in the industry tools that are updated for the ever-emerging threats that are present in the technology industry.

Below are some of the intrusion detection and control protocols KNOWiNK has deployed to protect the ePulse system for outside attacks and also the massive increase in load on Election day that thousands of devices can bring against the system. Intrusion detection and control protocols:

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

sales@knowink.com · 855.765.6723 · www.knowink.com · 2111 Olive Street, St. Louis, MO 63103

encryption standards and supported by industry leading AWS network teams.

AWS Shield - All traffic passes through Amazon's "Shield" product which provides both detection and mitigation of DDoS attacks.

Firewall - Once through Shield, traffic is passed through a firewall. Only ports 80 and 443 are open.

Virtual Private Cloud (VPC) - A virtual private cloud or "VPC" is a virtual isolated cloud environment which allows for all server and database resources to be isolated from the public internet. All traffic must first flow through a load balancer and firewall which then divides the traffic to the proper application server. Due to the isolated nature of the VPC even if an attacker had the IP address of an individual server, he or she could not connect to it.

Application Load Balancer - Once in the VPC, traffic is distributed using an AWS application load balancer to maintain high availability and scalability of internal resources. Application servers are hosted in differing availability zones, to ensure reliability if some external event were to affect a single availability zone.

Autoscale Groups - All application servers are assigned to auto scaling groups, which will automatically increase the number of running servers depending on demand. This allows for increased load during peak times (Election Day) and also decreases cost during down times. Autoscale groups combined with load balancers also mitigate DDoS attacks because server instances can scale automatically to handle increased load.

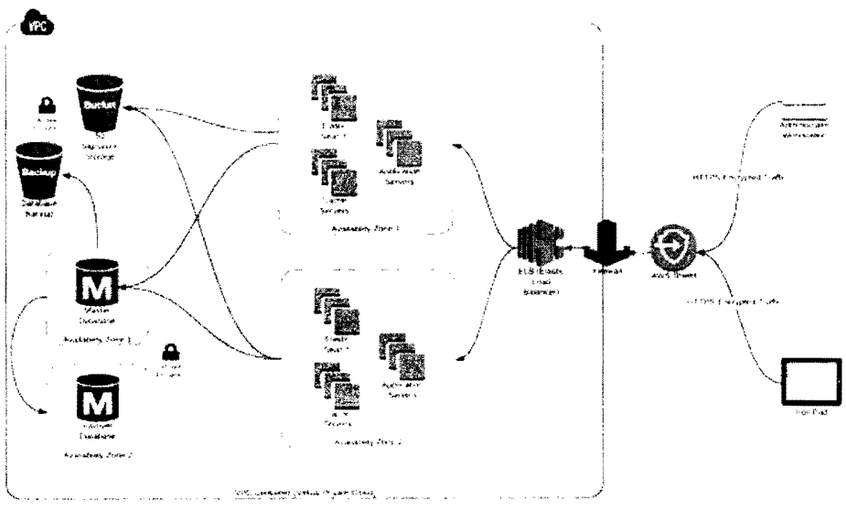
Security Groups - All AWS resources are assigned to a security group which defines which other resources can connect to them. This means for sensitive systems like the database server, only resources with a pre-authorized security group may connect to it.

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.

Amazon KMS - Amazon Key Management Service (KMS) is used to store all encryption keys that are used to encrypt all data within AWS. 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.



Centers for Information Security Benchmarks - KNOWiNK has hardened our systems to the Centers for Information Security (CIS) benchmarks for both the AWS account and the operating systems utilized by the application server instances.

The AWS account is hardened (where feasible) to Level 1 of the CIS Foundation Benchmarks for Amazon Web Services. These requirements set forth stringent application controls which increase the security of the AWS system utilized by KNOWiNK.

More information can be found here: https://d0.awsstatic.com/whitepapers/compliance/AWS_CIS_Foundations_Benchmark.pdf

The Ubuntu operating system utilized 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 here: https://learn.cisecurity.org/benchmarks

Built-in access control methods and login access levels - to secure and prevent unauthorized access to or dissemination of sensitive or confidential voter information, ePulse and Poll Pad employ comprehensive security access controls throughout the system. In ePulse, administrators may add users at will and assign those users to a specific access control level that permits users to perform authorized functions. For security purposes, Administrators are not allowed to set a user's password so that no person will know a user's password other than the user him or herself. Users receive an email with a link to create a secure password. The default password requirements are a minimum of 12 characters with at least 3 of the 4 character types: uppercase letters, lowercase letters, symbols, or numbers. These minimum requirements are changeable upon request. In addition, Multi Factor Authentication is available upon request.

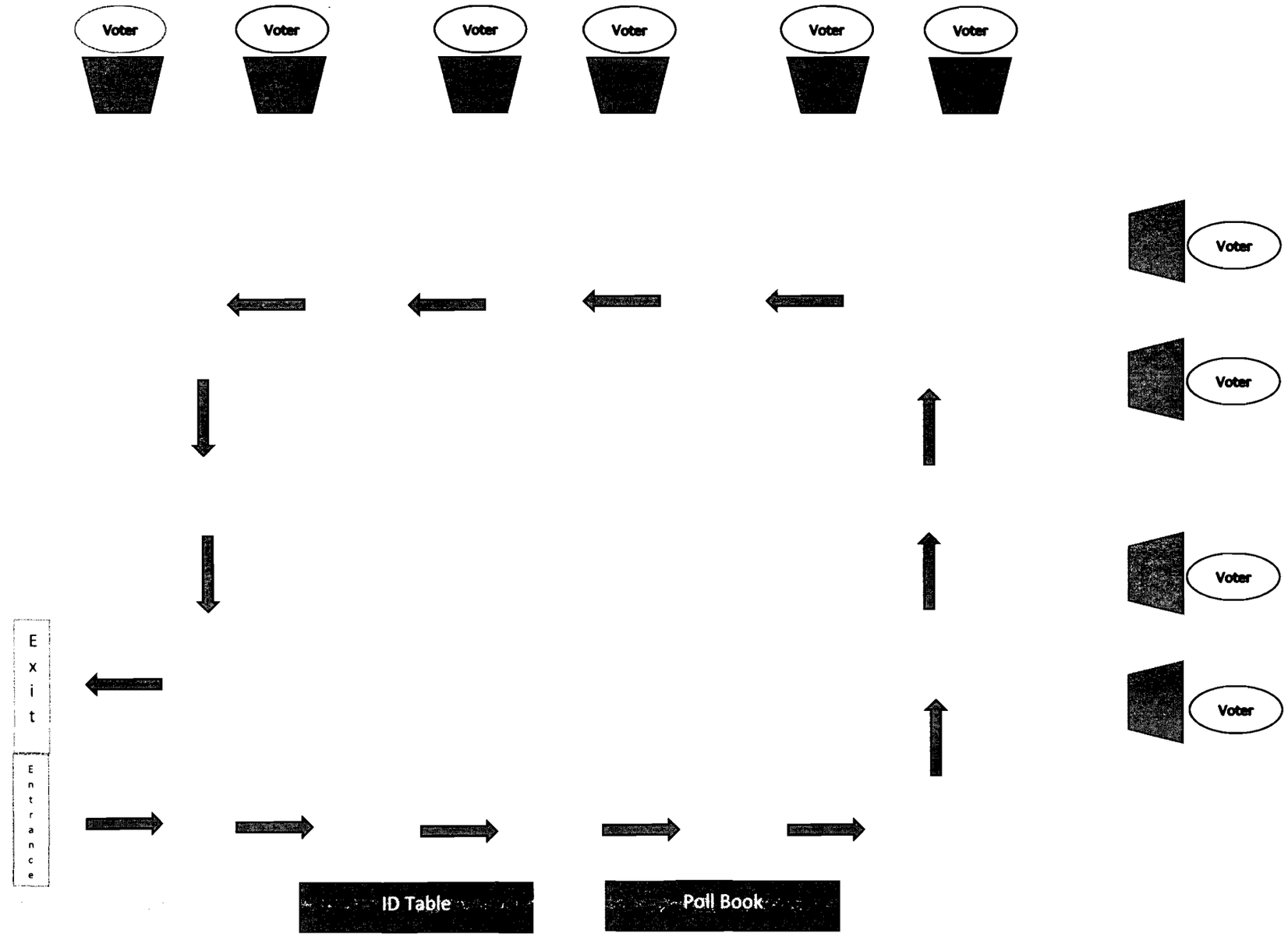
Users may be restricted from viewing certain sections or may be restricted to read only access to certain sections and features. Only Administrators with proper privileges can change a user's access level. All changes are logged to the system for review.

Poll Pad restricts access through a series of logins. Basic functions are optionally controlled by a base poll worker authentication. More advanced functions can be enabled by entering a supervisor or override password. Virtually every tap on the Poll Pad screen

is logged to the device and is available to export for post analysis.

Restricted External Devices - Poll Pad does not require the use of USB or removable memory cards for use. Apple inherently blocks removable memory from being connected to an iPad. KNOWiNK has developed a secure device, known as "iSync," that allows for data transfer to and from the Poll Pad application. In order to connect to our application, the device has been certified by Apple and issued a certificate by Apple that allows it to communicate with the Poll Pad application. All data included on the iSync drive is fully encrypted using 256 bit AES encryption and is validated by a certificate stored on the keychain of the iOS device. While this device is available and can make the Poll Pad easier to use, especially when a quick and reliable network connection is not available, it is not required for use.

Data Encryption - All data stored in both Poll Pad and ePulse is encrypted in transit and at rest. Poll Pad utilizes built in iOS encryption to encrypt the application and all data contained within. Certified by NIST to FIPS 140-2, the iOS operating system utilizes 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 utilizes 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. And, all databases utilize AWS powered encryption with encryption keys stored in the AWS key management service.


Voter
Voter
Voter
Voter
Voter
Voter
Voter
Voter
Voter
Voter
Exit
Entrance
ID Table
Poll Book

201701762 RESO $0.00
08/22/2017 08:44:33A 1 PGS
Wanda Taylor
Fountain County Recorder IN
Recorded as Presented

Resolution 2017-30

A RESOLUTION APPROVING THE DESIGNATION OF FOUNTAIN COUNTY AS A VOTE CENTER COUNTY

WHEREAS, Indiana Code 3-11-18.1 allows counties to adopt the vote center model and,

WHEREAS, the County Council of Fountain County approves the designation of Fountain County as vote center county and,

WHEREAS, the county election board has the responsibility for properly drafting a vote center plan for Fountain County, which will take effect upon unanimous vote of the county election board and having the plan is properly filed with the Indiana Election Division;

BE IT SO RESOLVED BY THE COUNTY COUNCIL OF FOUNTAIN COUNTY that Fountain County is approved to operate as a vote center county, upon the required approval and filing of the county vote center plan.

COUNTY COUNCIL OF FOUNTAIN COUNTY

"AYES"	"NAYS"
NAME	NAME
NAME	NAME
NAME	NAME
NAME	NAME
NAME	NAME
NAME	NAME
NAME	NAME

Adopted this 21st day of August, 2017

ATTEST: Brenda Hardy
Fountain County Auditor

This instrument prepared by Teryl D. Martin, Fountain County Attorney, Covington, Indiana.

I affirm under the penalties of perjury I have taken reasonable care to redact each Social Security number in this document, unless required by law. /s/Teryl D. Martin

201701679 RESO $0.00
08/07/2017 12:31:13P 1 PGS
Wanda Taylor
Fountain County Recorder IN
Recorded as Presented

Resolution 2017-30

A RESOLUTION APPROVING THE DESIGNATION OF FOUNTAIN COUNTY AS A VOTE CENTER COUNTY

WHEREAS, Indiana Code 3-11-18.1 allows counties to adopt the vote center model and;

WHEREAS, the County Board of Commissioners of Fountain County approves the designation of Fountain County as vote center county and;

WHEREAS, the county election board has the responsibility for properly drafting a vote center plan for Fountain County, which will take effect upon unanimous vote of the county election board and having the plan is properly filed with the Indiana Election Division;

BE IT SO RESOLVED BY THE BOARD OF COMMISSIONERS OF FOUNTAIN COUNTY that Fountain County is approved to operate as a vote center county, upon the required approval and filing of the county vote center plan.

BOARD OF COMMISSIONERS OF FOUNTAIN COUNTY

"AYES"	"NAYS"
NAME	NAME
NAME	NAME
NAME	NAME

Adopted this August of 7, 2017

ATTEST: Brenda Hardy
Fountain County Auditor

This instrument prepared by Teryl D. Martin, Fountain County Attorney, Covington, Indiana.

I affirm under the penalties of perjury I have taken reasonable care to redact each Social Security number in this document, unless required by law. /s/ Teryl D. Martin