MONITORING MADE EASY

Computer Security Policy Audits

Audit and verify field force compliance with your computer security policies without adding to the workload of your current staff.

Field force compliance with your written policies is an important component in keeping your reps, their clients, and the Broker-Dealer protected from loss and litigation. Unfortunately, in today's world, it is a number one priority, along with the ten other number one priorities you have on your plate.

Auditing and the necessary follow-up monitoring of field force computers can prove burdensome to three areas in a Broker Dealer: Audit, Compliance, and IT. Our system allows you to outsource these tasks. Using our sophisticated and efficient tools we identify the computers which fail to meet your policies, provide a gap analysis to be used to bring the offending computer into compliance and monitor the system to verify it has been brought into compliance.

For Your Auditors

Your auditors no longer need to spend time analyzing the status of each computer trying to figure out if they are compliant. An area many Auditors feel may be a little outside their area of expertise. The Auditor receives a comprehensive, easy to read report for each computer in the office, which clearly delineates any area of failure for inclusion in their report.

For Your Compliance Department

Our team follows up with the field office to cover any gaps found in their adherence to your policies. Your secure portal identifies any offices not making the necessary progress. Usually, a quick email or call is all that's required to get the process back on track. Concentrating only on the occasional laggard frees your compliance to focus on other tasks.

For Your Advisors

As part of their business relationship, the Advisor must collect and utilize their clients personal and private information. We take the responsibility to protect that information very seriously. Furthermore, we provide ongoing training and needed tools for the Advisor to use to communicate, to their clients, how they are safeguarding their private information. In turn, deepening trust and cementing the relationship.

For Your IT Department

Once you've communicated your specific policies to us, we take it from there. Your IT group will not have to discuss any of the policies or requirements with the field offices or their outsourced IT support organizations, we take care of all that for you. For those field offices who don't have access to either internal or external resources, we can provide remote support supplied by IT professionals familiar with your requirements and the needs of a small field office.

Ready to **transform your operations**?
Visit docupace.com for more information.

OUR SAFEGUARDS	
FUNCTION	**ACTIVITIES**
IDENTIFY	We have identified and maintain a list of information and information technology assets. The purpose is to ensure the information and assets we control align with our business objectives and we can protect the confidentiality, integrity and availability of these assets. We have evaluated cyber security risks and used these to develop our policies and procedures.
PROTECT	We limit access to information to only those with a clear need to know. We provide ongoing training and reminders to all staff to be mindful of cyber security risks. We maintain and patch systems to reduce vulnerabilities. We have implemented firewalls, anti-malware, and encryption technologies to prevent misuse or information exposure.
DETECT	We actively monitor systems to detect unexpected or unusual activity. Suspicious events are investigated and reported for investigation.
RESPOND	We promptly report suspicious events and engage appropriate service providers and authorities to determine cause and impact. Post incident reviews are conducted to provide opportunities for improvement.
RECOVER	Backups are maintained to allow prompt restoration of systems.

Deployment

The process couldn't be simpler. Provide us the list of Advisors you want to on-board and we take care of them getting the reporting agent installed on the appropriate devices.

For Your Bottom Line

In most cases, the cost of our service is born by the field office with the computers which failed to meet the policy requirements.