KEYLOGIC
Unlock & Empower

Information Assurance

Protecting Sensitive Data

Does your organization have access to large data sets of sensitive information? From classified information housed by Defense, Intelligence, and Homeland Security agencies to personal data such as health documents, tax records, or credit card account numbers, sensitive information must be protected from three types of security threats: (1) theft, internal intrusion, and improper handling, (2) external cyber attacks, and (3) disasters (natural and man-made).

Think of information assurance (IA) as a bit like insurance—without it, the losses to your organization could be irreparable.

To guard against improper handling of information, IA addresses the overlapping frameworks of policies and procedures, people, and technology. KeyLogic's IA experts make recommendations to establish policies on appropriate use and storage of data; to be sure that the right people and *only* the right people have access to sensitive information; and to put technological systems in place to act as a safety check. KeyLogic designs and builds systems that implement safe security processes. For example, we are building a system for a major credit card company to safeguard credit card information.

To guard against data loss from a flood, tornado, or earthquake, KeyLogic makes recommendations about security hardening, continuity of operations, and disaster recovery. For example, we encourage our clients to follow our lead in having two servers geographically separated from each other so that a single disaster is unlikely to shut down operations.

Whether your organization protects national security information or sensitive personal information, look to KeyLogic for subject matter expertise in information assurance. We can help you set up the following safeguards:

- Policies and procedures on the appropriate use and storage of information
- Technological systems to act as an audit trail of who is viewing and using data—and ensuring they have a "need to know"
- Internal controls to prevent fraud
- Security hardening, including the physical strength of the building housing the data and an uninterruptible power supply to protect against data loss due to a localized power outage
- Multiple servers in separate locations to ensure continuity of operations

To learn more about how KeyLogic can help your organization protect sensitive information, please contact us today at 888.204.9649.