LIS SOLUTIONS

SECURITY MONTHLY NEWSLETTER

FEBRUARY 2024

DOD INFORMATION SECURITY PROGRAM:

At LIS Solutions, an Information Security Program designed to protect and safeguard classified information is just as important as a DoD Security Program.

An effective DoD Information Security Program is an appropriate way to classify, protect, and share information. In addition, it provides a way to apply applicable downgrading and appropriate declassification instructions and use authorized destruction methods for official information which requires protection in the interest of national security.

In an Information Security Program, you have appropriate guidelines for Classification, Safeguarding, Dissemination, Declassification, and Destruction of classified information.

- Classification is the act or process by which information is determined to require protection against unauthorized disclosure and is marked to indicate its classified status.
- Safeguarding refers to using prescribed measures and controls to protect classified information.
- Dissemination refers to the sharing or transmitting of classified information to others who have authorized access to that information.
- Declassification is the authorized change in status of information from classified to unclassified.
- Destruction refers to destroying classified information so that it can't be recognized or reconstructed.

Classified information is not only in the form of paper documents, but it can also be in electronic and verbal forms too. Regardless of what form it is in, classified information must be appropriately protected.

An effective execution of a robust information security program gives equal priority to protecting information in the interest of national security and demonstrating a commitment to transparency in Government. It also requires an accurate and accountable application of classification standards and routine, secure downgrading, and declassification of information no longer requiring the same level of protection. You play a pivotal role within the DoD workforce, and we all play a vital part in ensuring the effectiveness of the DoD Information Security Program.

Overall, our country's national security depends on protecting classified materials against unauthorized disclosure, which could inhibit our national defense and adversely affect our foreign relations.

For information to be eligible for classification, it must be official government information that is owned by, produced by, produced for, or under strict control of the U.S. Government, which means the U.S. Government has the authority to regulate access to that information. Therefore, if materials are controlled by the U.S. Government and disclosure of the information could cause damage to national security, it may be classified.

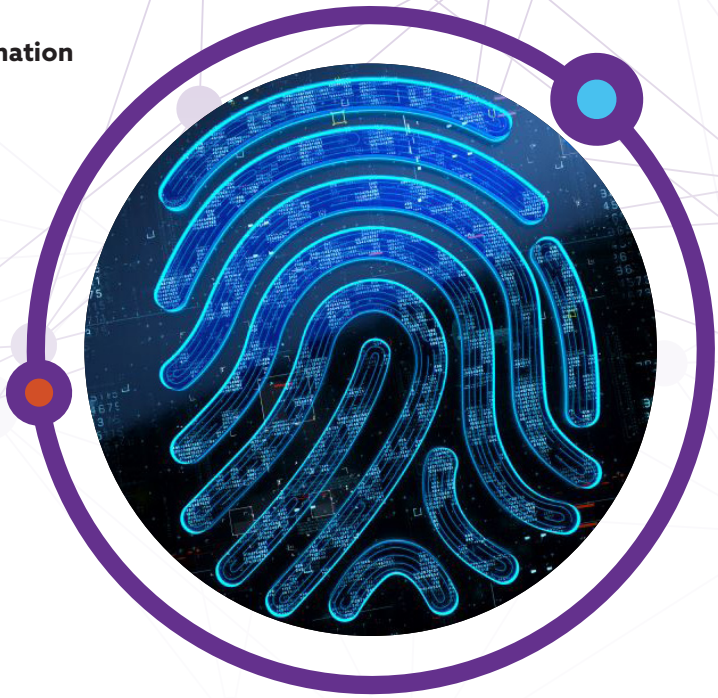
LIS Solutions
Analyze. Inform. Empower.

718-237-8919 • info@lissol.com

EMERGENCY PLANNING STEPS:

Now, let's look at the four critical steps to developing an information security emergency plan:

1. Identify the threats.
2. Assess the risks.
3. Determine possible protection strategies.
4. Develop an emergency plan.



Emergency plans are not all the same. They must be developed based on the variety of threats that your facility encounters. The level of detail in the plan is dependent upon your local threats, the level of assessed risks, and other circumstances. Your facility will keep a plan as simple as possible and thoroughly communicate your plan throughout your organization. As with any plan your facility must continually test it and be sure to utilize the results of the testing to identify problems and make the necessary adjustments to improve your plan.

Read the Information Security article below at your leisure:

Borromeo, M. (2024, January 11). How Small Businesses Can Help Efficiently Mitigate Information Security Risks. **https://martechseries.com/mts-insights/guest-authors/how-small-businesses-can-help-efficiently-mitigate-information-security-risks/**

LIS Solutions
Analyze. Inform. Empower.
718-237-8919 • info@lissol.com