HADMÉRNÖK

VII. Évfolyam 1. szám - 2012. március

Kuris Zoltán
zoltan.kuris@bm.gov.hu

THE PROTECTION OF CLASSIFIED INFORMATION, COMPLEX SUBSYSTEMS

Absztrakt/Abstract

Jelen cikkben a szerző ismerteti a hazai nemzeti és külföldi minősített adatokat kezelő komplex rendszer személyi, fizikai, adminisztratív és elektronikai védelemre vonatkozó követelményeket, a megvalósításukkal kapcsolatos dilemmákat, valamint javaslatokat fogalmaz meg a még nem szabályozott területein elveiket, módszereiket és eszközeiket illetően.
A minősített adatokat kezelő rendszerekben kezelt minősített adat bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása komplex védelmi intézkedéseket igényel a rendszer teljes életciklusában. Ezen intézkedések csak akkor lehetnek kellően hatékonyak, költségek szempontjából is optimalizáltak, ha azokat a biztonsági kockázatokkal arányosan tervezik és implementálják.

In this article the author demonstrates the personnel, physical, administrative and electronic protection requirements of national and international classified data handelingv complex systems, and, the design-related dilemmas about their implementation, in additon draws up recommendations about their principles, methods and instruments for the unregulated areas.
The confidentiality, integrity and availability, of classified information that is handled in systems dealing with classified information, require complex protective measures during the entire life-cycle of the system. Such measures should be enough efficient and cost-efficient if they are designed and implemented regarding of the security risks.

Kulcsszavak/Keywords: *minősített adatok, zárt terület, kommunikáció biztonság, bizalmas adat, információ biztonság, nemzeti minősített ada, szükséges tudni, biztonsági terület, korlátozott terjesztésű adat ~ classified information, closed area, communications intelligence, confidential, facility, information security, national security information, need-to-know, restricted area, restricted data*

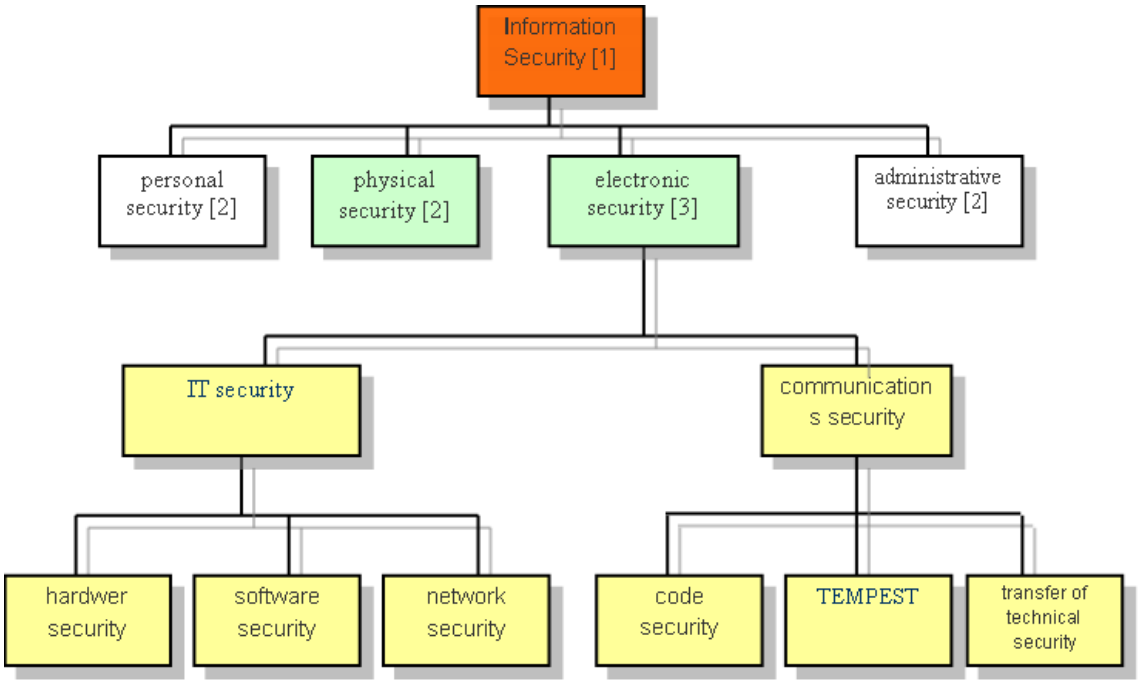
1. INTRODUCTION

The statutory rules of the government decree [1].

The government dercree of safety includes the following areas of expertise [2; 3]:

- personal security
- physical security
- administrative security
- electronic security

The safety provider secures the operation of the system in all area. The security system is made up of subsystems:



1. figure. the comlex information security systems

2. PERSONAL SAFETY (USER AUTHORIZATION)

A security clearance is a privilege, not a right. When the user accepts the privilege of access to classified information, someone also accepts the responsibilities of this privilege. The user's responsibility is the classified information protecting, which means a LIFELONG obligation. It continues afterwards someone no longer has an active security clearance. The Nondisclosure Agreement is signed when accepting your clearance, which is a legally binding agreement between the user and the state. If someone do not comply with procedure of classified information, the agremment's legal sanctions are executed beacause of breaching this contract. The intentional violation - with purpose to enrichment- may be prosecuted. This agreement assign the legal right of any payments to the state Government, royalties or other benefits, which someone could receive as a result of unauthorized disclosure of classified information.The signed Nondisclosure Agreement is the only form to hold on file long after you retire.

The personnel security is an application of measures to ensure that certified data is only known by individuals who has [4]:

A need-to-know, been security cleared to the relevant level, where appropriate, and been briefed on their responsibilities.

The personnel security clearance procedures shall be designed to determine the individual's loyalty, trustworthiness and reliability.

[1]That sums it up. The individual – not our foreign adversaries or competitors – is the principal source of the problem, but the person can also become the solution. Anybody who holds a security clearance is the first line of defense against espionage and other loss of sensitive information. If everybody fulfill our responsibilities, we have the power to protect our national security and economic interests.

3. NEED-TO-KNOW

Need-to-know is difficult to implement as it conflicts with our natural desire to be friendly and helpful. It also requires a level of personal responsibility that many of us find difficult to accept. The importance of limiting sensitive information is who have a need to know is underscored. every time a trusted insider is found to have betrayed that trust. The security clearance does not give approved access to all classified information. It gives access only to that Information at the same or lower level of classification which the level of the clearance granted; AND that you have a "need-to-know" in order to perform your work. Need-to-know is one of the most fundamental security principles. The practice of need-to-know limits the damage that can be done by a trusted insider who has ill-will. The failures of the need-to-know principle implementing have contributed greatly the damage caused by a number of recent espionage cases.

Need-to-know imposes a dual responsibility on all the other authorized holders of classified information. When doing your job, you are expected to limit your requests for information to that which you have a genuine need-to-know. Under some circumstances, the user may be expected to explain and justify your need-to-know when asking others for information. Conversely, the user has to ensure that anyone, - who get the classified information - has a legitimate need to know that information. The user liable for asking the other person about the sufficient information to make a well-founded decision about their need-to-know. On the other hand the recipient person is obliged to justify their need-to-know. The user is expected to refrain from discussing classified information in hallways, cafeterias, elevators, rest rooms or smoking areas where the discussion may be overheard by persons who do not has a need-to-know the subject of conversation. The user is also obliged to report to the user's security office any co-worker who repeatedly violates the need-to-know principle.

4. CERTIFICATION PROCESS

The original classification is the initial determination which define the requires of protection.

Only the Government officials, whom this authority has been delegated in writing and who have been trained in classification requirements, have the authority for original classification. Original classification authorities issue security classification guides, that others use in making derivative classification decisions. Most government employees and contractors make derivative classification decisions. Derivative classification is the act of classifying a specific item of information or material on the basis of an original classification decision by an authorized original classification authority. The source of authority for derivative

[1] Pogo, a popular cartoon character from the 1960s, coined an oft-quoted phrase:
"We have met the enemy, and he is us."

classification ordinarily consists of a previously classified document or a classification guide issued by an original classification authority.

5. CLASSIFICATION LEVELS

The competent authorities shall ensure the appropriately classification, clearly identifcation (as classified information) and the classification level for only as long as necessary. Classified information can not be downgraded or declassified nor shall any be modified or removed without the prior written consent of the originator [4].

Information that must be controlled to protect the national security, who is assigned one of four levels of classification, as follows:

- TOP SECRET information is an information which is disclosed without authorization, could reasonably be expected to cause exceptionally grave damage to the national security.
- SECRET information is an information which is disclosed without authorization, it could reasonably be expected to cause serious damage to the national security.
- CONFIDENTIAL information is an information which is disclosed without authorization, it could reasonably be expected to cause damage to the national security.
- RESTRICTED information is an information which is disclosed without authorization, it could be disadvantageous to the interests of the national security.

Any approved holder of classified information - who believes the information is classified improperly or unnecessarily, or that current security considerations justify downgrading to a lower classification or upgrading to a higher classification, or that security classification guidance is improper or inadequate - is encouraged and expected to challenge the classification status. Government employees should pursue through such actions to establish agency procedures that protect individuals from retribution for bringing such actions, and to provide an opportunity for review by an impartial official or panel. And it also provide the right to appeal to the Interagency Security Classification Appeals Panel.

6. MARKING CLASSIFIED INFORMATION

Physically marking classified information with appropriate classification and control markings serves to warn and inform holders of the degree of protection required. Other notations aid in refering the derivative of the classification actions and it also facilitates the downgrading or declassification. On the other hand the marking of the classified information and material should be clearly convey the level of classification assigned, the portions that contain or reveal classified information, the period of time protection is required, and any other notations required for protection of the information or material.

Below I summarize of the most commonly used document control markings. More detailed information is available via the Internet from a variety of sources.

6.1. Overall Classification Markings

The overall (i.e. highest) classification of a document is marked at the top and bottom of the outside cover (if there is one), the title page (if there is one), the first page, and on the outside of the back cover (if there is one) or on the back side of the last page.

Each interior page, which contains classified information, is marked on the top and bottom with „the overall (i.e., highest) classification of the page” sign. Each unclassified interior page is marked 'Unclassified" sign at the top and bottom. Interior pages which have „For Official

Use Only" sign, are have to be marked only at the bottom. Blank pages do not require any markings.

Attachments and annexes may be separated from the basic document. In this case they should be marked as if they were separate documents.

Additionally, every classified document must show two relevant information on the face of the document, the one of them is the name of the agency or office who classified the documantion, and the other is the date of creation process. This information must be clear enough to allow someone to receive the document, or to contact the preparing office if questions or problems arise about classification process. The computer files must be marked by appropriate headers and footers to ensure the applicable classification and associated markings are appeared in the transmitted or printed version as well. All removable storage media and devices such as diskettes, CD-ROMs, cassettes, magnet tape reels, etc. must have an outer label about the appropriate markings. Each slide must be marked on the slide itself or slide cover, as well as on the image that is projected.

7. HANDLING CLASSIFIED INFORMATION

As an approved custodian or user of classified information, has an personally responsible for the protection and control of this information. The user must safeguard this information at all times to prevent loss or compromise, unauthorized disclosure, dissemination, or duplication. Unauthorized disclosure of classified material is punishable under the criminal regulations or legislation organizational policies.

The security officer or supervisor briefs the specific rules for handling classified information which is attach the special organization. Here are some standard procedures that apply to everyone.

Classified information that is not safeguarded in an approved security container shall be constantly under the control of a person having the proper security clearance and need-to-know. An end-of-day security check should ensure that all classified material is properly secured before closing for the night.

If someone find a classified material which is left unattended (for example, in a rest room, or on a desk), it should be the user's responsibility, because the user has to ensure that the material is properly sprotected. In this case someone has to stay with the classified material and notify the security office. If this is not possible, the document or other material should be taken to the security office. The supervisor, or another person is authorized to access to this type of the information, or, if necessary, they can lock the material in your own safe overnight.

The classified material shall not be taken home, so nobody is allowed to work on classified material at home.

Classified information shall not be put in the waste basket. It must be placed in a designated container to overwhelm the classified documents by an approved method of destruction such as shredding or burning.

E-mails and the Internet create many opportunities for inadvertent disclosure of classified information. Before an user send an e-mail, post to a bulletin board, publish anything on the Internet, or add to an existing Web page, they must be absolutely certain there is none of the information is classified or sensitive unclassified information. Be familiar with the organization's policy for the use of the Internet. Many organizations require prior review of ANY information which is put on the Internet.

Classified working papers such as notes and rough drafts should be dated when it is created. They are marked with the overall classification and with the annotation "Working Papers," and disposed of with other classified waste when no longer needed.

Computer diskettes, magnetic tape, CDs, carbon paper, and used typewriter ribbons may create a problem about the security checking. As visual examination does not readily reveal whether the items contain classified information. To reduce the possibility of error, some offices treat all such items as classified even though they may not necessarily contain classified information.

Foreign government material should be stored and access controlled generally in the same manner as national. Inspite of the equivalent classification, the classified materials must be separated.

The Top Secret information is subject to continuing accountability.The official's Top Secret control are designated to receive, transmit, and maintain access and accountability records for Top Secret information. When information is transmitted from one Top Secret control official to another, the receipt is recorded and a receipt is returned to the sending official. Each item of Top Secret material is numbered in series, and each copy is also numbered.

8. APPROPRIATE USE OF COMPUTER SYSTEMS

Information Assurance (hereafter: IA) in the field of communication and information systems is the confidence that such system will protect and handle the information, and it will operate as it necessary, under the control of legitimate users. Effective IA shall ensure appropriate levels of confidentiality, integrity, availability, non-repudiation and authenticity. IA shall be based on a risk management process.

The „Communication and Information System" means any system enabling the handling of information in electronic form. A communication and information system shall contain the entire assets - including the infrastructure, organisation, personnel and information resources [4] - required to operate,.

Misuse of an automated information system is sometimes illegal, often unethical, and always reflects poor judgment or lack of care in following security rules and regulations. Misuse may create security vulnerabilities or cause damage to important information. A pattern of inability or unwillingness to follow rules for the operation of computer systems raises serious concerns about an individual's reliability and trustworthiness. As we store more and more information in computers data bases, and as these data bases become more closely linked in networks, more people have broader access to more information than ever before. The computer technology has magnified many times the ability of a careless or disaffected employee to cause severe damage.

Many aspects of computer use are governed by your organization's policy rather than by government regulation. Many government agencies and defense contractors specify the security procedures and prohibited or inappropriate activities discussed below.

8.1. Security Rules

The following are basic rules for the secure use of the computers.

- Do not enter into any computer system without authorization. Unauthorized entry into a protected or compartmented computer file is a serious security violation and is probably illegal. It can be a basis for revocation of your security clearance. Whether motivated by the challenge of penetrating the system or by simple curiosity to see what is there, unauthorized entry is a deliberate disregard for rules and regulations. It can cause you to be suspected of espionage. At the bare minimum, it violates the need-to-know principle and in some cases is an invasion of privacy.

- Do not store or process classified information on any system not explicitly approved for classified processing.
- Do not attempt to circumvent or defeat security or auditing systems without prior authorization from the system administrator, other than as part of a system test or security research authorized in advance.
- Do not install any software on your computers without the approval of your system administrator.
- Do not use another individual's user ID, password, or identity.
- Do not permit an unauthorized individual (including spouse, relative or friend) access to any sensitive computers network. Do not leave sensitive but unclassified work materials on a home computers to which other persons have access.
- Do not reveal your password to *anyone* -- not even your computers system administrator.
- Do not respond to any telephone call from anyone whom you do not personally know who asks questions about your computers, how you use your computers, or about your user ID or password.
- If you are the inadvertent recipient of classified material sent via e-mails or become aware of classified material on an open bulletin board or web site, you must report this to the security office.
- Do not modify or alter the operating system or configuration of any system without first obtaining permission from the owner or administrator of that system.
- Do not use your office computers system to gain unauthorized access to any other computers systems.

8.2. Inappropriate Use

Many offices permit some minimal personal use of official equipment when such personal use involves minimal expense to the organization. This is performed on someone's personal non-work time, which does not interfere with the mission of the office, and does not violate standards of ethical conduct.

The following activities are considered to be misuse of office's equipment:

- The creation, downloading, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials can cause to be fired.
- Annoying or harassing another individual, for example through uninvited e-mails of a personal nature or using lewd or offensive language can cause to be fired.
- Using the computers for commercial purposes or in support of "for-profit" activities or in support of other outside employment, business activity (e.g., consulting for pay, sales or administration of business transactions, sale of goods or services), or gambling.
- Engaging in any outside fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity.
- The creation, copying, transmission, or retransmission of chain letters or other unauthorized mass mailings.
- Any activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include hate speech or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.
- Use for posting office information to any external newsgroups, chat rooms, bulletin boards, or other public forums without prior approval.

- Any personal use that could cause congestion, delay, or disruption of service to any office equipment. This includes sending pictures, videos, or sound files or other large file attachments that can degrade computers network performance.
- The unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information. This includes copyrighted computers software; other copyrighted or trademarked materials or materials with intellectual property rights (beyond fair-use); privacy information; and proprietary data or export-controlled data or software.

9. E-MAIL

There are two big problems with e-mails; one of them is the increased risk of accidental security compromise; the other is sending inappropriate materials by e-mail, which has caused many people to be fired.

9.1. Security Risks with E-Mail

As a result of the Internet and e-mail, there has been a sharp increase in security incidents involving the accidental disclosure of classified and other sensitive information. One common problem occurs always when individuals download a seemingly unclassified file from a classified system, and then fail to carefully review this file before sending it as an attachment to an e-mail message. Too often, the seemingly unclassified file actually has some classified material or classification markings that are not readily apparent when the file is viewed on line. Sending such material by e-mail is a security violation even if the recipient has an appropriate security clearance, as e-mail can easily be monitored by unauthorized persons.

More important, even if the downloaded file is really unclassified, the electronic version of that file may have recoverable traces of classified information. This happens because data is stored in "blocks." If a file does not take up an entire block, the remainder of that block may have recoverable traces of data from other files. The administrator system must follow an approved technical procedure for removing these traces before the file is treated as unclassified.

Some organizations have found to lock their computers drives to prevent any downloading of files from the classified system. If necessary to download and retransmit an unclassified file from a classified system, the file must be downloaded and processed by the system administrator to remove electronic traces of other files before it is retransmitted.

9.2. Inappropriate Materials

Sending e-mail is like sending a postcard through the mail. Just as the mailman and others have an opportunity to read a postcard, network eavesdroppers can read your e-mail as it passes through the Internet from computer to computer. E-mail is not like the secrecy of correspondence, where your privacy rights are protected by law.

The courts have repeatedly sided with employers who monitor their employees' e-mail or Internet use. A 2005 survey found that 63% of corporations with 1,000 or more employees either employ or plan to employ staff to read or otherwise analyze outbound email. 27% of the companies reported terminating an employee due to email misuse during the previous year. 35% investigated a suspected email leak of confidential information during the past year. In addition to protection of their intellectual property, companies were concerned about compliance with financial disclosure regulations.

Organizations also monitor email to protect themselves against lawsuits, as the organization can be held liable for abusive, harassing, or otherwise inappropriate messages sent over its computers network.[2]

10. SECURITY OF HARD DRIVES

Secrets in the computers require the same protection as secrets on paper. This is because information can be recovered from a computers hard drive even after the file has been deleted or erased by the computers user. It is estimated that about a third of the average hard drives contains information that has been "deleted" but it is still recoverable.

When someone deletes a file, most computers operating systems delete only the "pointer", which allows the computer to find the file on the hard drive. The file itself is not deleted until it is overwritten by another file. This is comparable to deleting a chapter heading from the table of contents of a book, but not removing the pages on which the chapter is written. Some networks may be configured to "wipe" or purge the hard drive when information is deleted, but most are not.

Computers on which classified information is prepared must be kept in facilities that meet specified physical security requirements for processing classified information. If necessary to prepare classified information on a computer in a non-secure environment, erybody has to use a removable hard drive or laptop that is secured in an approved safe when it is not in use. Alternatively, they can use a typewriter.

11. COMPUTER PASSWORDS

Passwords are used to authenticate an individual's right to have access to certain information. A password could be use only personally. Lending it to someone else is a security violation and may result in disciplinary action against both parties. Never disclose your password to anyone. Memorize it – do not put it in writing. If someone leave the terminal unattended for any reason, log off or use a screen lock. Otherwise, someone else could use the computer to access information, they are not authorized to have. Someone will be held responsible if anybody else uses other password in connection with a system transaction.

As hackers and scammers develop more clever ways to steal passwords, it becomes more important that passwords be changed regularly. Use a password with at least six and preferably eight characters and consisting of a mix of upper and lower case letters, numbers, and special characters such as punctuation marks. This mix of various types of characters makes it more difficult for a hacker to use an automated tool called a "password cracker" to discover your password. Cracking passwords is a common means by which hackers gain unauthorized access to protected systems.

12. "SOCIAL ENGINEERING"

"Social engineering" is hacker-speak for conning legitimate computers users into providing useful information that helps the hacker gain unauthorized access to their computers systems.

---

[2] In the past couple of years, The New York Times fired 23 employees for exchanging off-color e-mails. Xerox fired 40 people for inappropriate Internet use. Dow Chemical fired 24 employees and disciplined another 230 for sending or storing pornographic or violent material by e-mail. Several years ago, Chevron Corp. had to pay $2.2 million to plaintiffs who successfully brought a suit of sexual harassment, in part because an employee sent an e-mail to coworkers listing the reasons why beer is better than women.

The hacker using social engineering usually poses as a legitimate person in the organization (maintenance technician, security officer, inexperienced computer user, VIP, etc.) and employs a plausible cover story to trick computer users into giving useful information. This is usually done by telephone, but it also may be done by forged e-mail messages or even in-person visits.

Most people have an incorrect impression of computers break-ins. They think they are purely technical, the results of technical flaws in computers systems which the intruders are able to exploit. However, the truth is that social engineering often plays a big part in helping an attacker slip through security barriers. Lack of security awareness or gullibility of computer users often provides an easy stepping stone into the protected system if the attacker has no authorized access to the system at all.

13. PROTECTING YOUR HOME COMPUTER

If someone access own office network from home or do work at home that is emailed to the office or brought to the office on any removable storage media. This can affect the security of the office network. If someone has an obligation to take standard procedures for protecting own home computer against viruses and other problems, it might be transmitted to own office network. These include installing a virus checker with automatic updates, installing a personal firewall, turning off or uninstalling any options that significantly increase security risk, and keeping the operating system of own computer up-to-date with security fixes as they become available.

14. SECURITY VIOLATIONS

A security violation or infraction is any breach of security regulations, requirements, procedures or guidelines, whether or not a compromise results. No matter how minor, any security infractions must be reported immediately to the security office so that the incident may be evaluated and any appropriate actions taken.

14.1. Deliberate Violation[3]

[6] Any deliberate violation of security rules or regulations is a significant concern, as it may indicate indifference toward national security or a general inability or unwillingness to abide by the security regulations.

Any deliberate revelation of classified or other protected information to any unauthorized person is a particularly egregious offense. Examples of this include:

- Leaking protected information to journalists or others in an effort to influence Government policy.
- Giving protected information to a private company or corporation to pursue some personal business interest or to pave the way for seeking a job there, or to help a relative or friend in their business even if not done for personal gain.
- Giving protected information to a friend or business associate just to impress them with one's importance.

[3] Naval Intelligence analyst Jonathan Jay Pollard passed several classified political and economic analyses to three different friends whom he felt could use the information in their business. Although Pollard hoped to get some benefit in return, his principal motive was simply to impress his friends with his knowledge and the importance of his work. Willingness to sacrifice security for minor personal gain indicates a degree of narcissism that is a serious concern. This attitude can be dangerous and may portend future problems. In Pollard's case, for example, his need to feel important and to have others validate that importance subsequently led him to volunteer his services to Israeli Intelligence. He is now serving a life term in prison.

14.2. Pattern of Negligence or Carelessness

[6] A pattern of routine security violations due to negligence, carelessness, inattention, or a cynical attitude toward security discipline is potentially disqualifying regardless of whether or not information was actually compromised.

14.3. Major Violations[4]

The significance of a security violation does not depend upon whether information was actually compromised. It depends on the intentions and attitudes of the individual who committed the violation.

Ability and willingness to follow the rules for protection of classified information is a prerequisite for maintaining your security clearance. Although accidental and infrequent minor violations are expected to deliberate or repeated failure to follow the rules is definitely not. It may be a symptom of underlying attitudes, emotional, or personality problems that are a serious security concern.

The following behaviors are of particular concern and may affect your security clearance:

- A pattern of routine security violations due to inattention, carelessness, or a cynical attitude toward security discipline.
- Taking classified information home, ostensibly to work on it at home, or carrying it while in a travel status without proper authorization.
- Prying into projects or activities for which the person does not have (or no longer has) a need to know. This includes requests for classified publications from reference libraries without a valid need to know, or any attempt to gain unauthorized access to computers systems, information, or data bases.
- Intoxication while carrying classified materials or that causes one to speak inappropriately about classified matters or to unauthorized persons.
- Deliberate revelation of classified information to unauthorized persons to impress them with one's self-importance.
- Copying classified information in a manner designed to obscure classification markings. This may indicate intent to misuse classified information.
- Making unauthorized or excessive copies of classified material. Going to another office to copy classified material when copier equipment is available in one’s own work area is a potential indicator of unauthorized copies being made.
- Failing to report requests for classified information from unauthorized individuals.
- Leaving a classified file or security container unlocked and unattended either during or after normal working hours.
- Keeping classified material in a desk or unauthorized cabinet, container, or area.
- Leaving classified material unsecured or unattended on desks, tables, cabinets, or elsewhere in an unsecured area, either during or after normal working hours.
- Reproducing or transmitting classified material without proper authorization.
- Losing one’s security badge.
- Removing classified material from the work area in order to work on it at home.
- Granting a visitor, contractor, employee or any other person access to classified information without verifying both the individual's clearance level and need-to-know.

[4] Storing classified information at home is **a** very serious concern as it may indicate current or potential future espionage. At the time of their arrest, many well-known spies were found to have large quantities of classified documents at their residences. [5] CIA spy Aldrich Ames had 144 classified documents at his home, while Edward Moore had 10 boxes of CIA documents at home. Of various Navy spies, Jonathan Pollard had a suitcase full of classified materials, Michael Walker had 15 pounds of classified material, while Samuel Morison had two portions of Navy documents marked Secret.

- Discussing classified information over the telephone, other than a phone approved for classified discussion.
- Discussing classified information in lobbies, cafeterias, corridors, or any other public area where the discussion might be overheard.
- Carrying safe combinations or computers passwords (identifiable as such) on you, writing them on calendar pads, keeping them in desk drawers, or otherwise failing to protect the security of a safe or computers.
- Failure to mark classified documents properly.
- Failure to follow appropriate procedures for destruction of classified material.

Failure to report a security violation is itself a security violation and may be a very serious concern!

15. CONCLUSION

Based on international experience which can demonstrate, that the protection of classified information has a lot of components. In this article I have highlighted some of these important areas. I find personal safety very important because it creates the foundation for the protection of classified information. I have written down the rating regulations from the field of administrative security because this is important. A need to know is a very important element of security. The ratings data management policy is explained to me, because it is an essential prerequisite for daily work. In the case of a breach of security, it is very important to minimize the damage, therefore the basic rules are described. Rated datas are produced and handled on modern computing devices in the 21st century._ The most important rules of electronic handling are described as well. As described, the above demonstrate that the most efficient way you can ensure classified information is to use safety areas in a coordinated way.

References:

[1] A minősített adat védelméről szóló 2009. évi CLV. törvény

[2] A nemzeti biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010.(III.26.) Korm. rendelet

[3] A minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010.(V.6.) Korm. rendelet

[4] COUNCIL DECISION of 31 March 2011 on the security rules for protecting EU classified information (2011/292/EU)

[5] SECURITY WITHIN THENORTH ATLANTIC TREATY ORGANISATION Corrigendum to C-M(2002)49 dated 17 June 2002Amendment 3

[6] http://www.dhra.mil/perserec/adr/handlinginfo/handlingtext.htm; (2012. 01. 06.)