Proposal for Data Protection, Information Security and Access Rights

(This document name is: „Data Protection, Information Security and Access Rights 2020“, normal text font used is Arial 11, paragraph line spacing Single, 6 pt. before and after)

Miodrag Perisic, MSEE, ICT Expert, “Support to the Justice Sector Reform” project

June 2020.

Funded by the European Union

Vladimir Polezhinovski, 22/12, Skopje, Republic of North Macedonia
Team leader Dr. Deville: +389 (0) 70 22 40 44
E-mail: deville@planet.gr

Project implemented by NIRAS and its consortium partner Planet

Table of Contents

Abbreviations:

ICT	Information and Communications Technology
PO	Prosecution office
ITIL	formerly an acronym for Information Technology Infrastructure Library, is a set of detailed practices for ICT service management (ITSM) that focuses on aligning ICT services with the needs of business.
ACCMIS	Current Automated Courts Case Management Information System, as implemented in all courts in North Macedonia
HW	Computer systems hardware, equipment used to perform IT activities
SW	Computer systems software, programs, applications and various utilities, run on hardware
Help Desk/Support	system providing help to both computer system users and ICT staff
CIO	Chief Information Officer, top managerial position in an organization, responsible for all information services, storage and safety
Server	a HW-based device, with processor, memory and storage, used for various computer processing functions, stored in racks with many connected servers inside

Executive Summary

This document, when completed, should become a part of the collection of different documents, proposals and frameworks, provided as the results of the specification of the Requested Services within the Terms of Reference (ToR), for the Component 3 (ICT) of the project “Support to the Justice Sector Reform”

This document, in this latest version dated June 2020, has been completed using all comments, additions and changes as proposed in the meantime by the members of the ICT Council, and as such is considered final version, ready for adoption by the ICT Council.

The document has been initially designed by the project consultant, ICT Expert, after which it has been shared with a number of ICT staff across the country, distinguished members of the ICT community both at the courts and prosecution offices, who provided additional, specific comments and details, to make it fully applicable and in line with the current situation in these organizations and their future needs and possible ICT-related directions.

Besides this, the document also took into account previously expressed opinions and suggestions, as documented in the report on the Open Space training, which took part in Skopje, by end January 2020, and included over 20 representative ICT staff from various courts and prosecution offices in North Macedonia (see later for more details)

This document is presenting a common approach to the implementation of the Information Security Policy, adjusted to the specific situation in North Macedonia justice institutions, such as the courts and prosecution offices. Wherever possible or applicable, short notes are inserted, with specific comments on situation with these institutions.

Towards the end, a specific set of measures to be taken in North Macedonia justice organizations will be proposed, based on inputs provided by the ICT Council and wider ICT community in these organizations.

1. Definition & Intro

Information Security Policy (ISP) is a set of rules enacted by an organization to ensure that all users or networks of the ICT structure within the organization’s domain abide by the prescriptions regarding the security of data stored digitally within the boundaries the organization stretches its authority.
An ISP is governing the protection of information, which is one of the many assets a corporation needs to protect. The present writing will discuss some of the most important aspects a person should take into account when contemplates developing an ISP. Putting to work the logical arguments of rationalization, one could say that a policy can be as broad as the creators want ICT to be: basically, everything from A to Z in terms of ICT security, and even more. For that reason, the emphasis here is placed on a few key elements, but you should make a mental note of the liberty of thought organizations have when they forge their own guidelines.

Results of the polling of opinions at the ICT Open Space training

At the Open Space Training session, which our project has organized by end January 2020, for the ICT Council members and other ICT staff from various judicial institutions in North Macedonia, the attendants have been asked to provide their opinions on necessary priority actions and initiatives on several topics. In regards to the topic “ICT Organization” these were their contributions:

1. Electronic exchange of information between various institutions within the system (current issues, activities, etc.); at the moment, this is done only at the meetings of the ICT Working Group, every 2-3 months;
2. Systematization & documenting of all ICT activities;

3. Creation of Help Desk/Support system for all ICT staff, for easy, available method of exchanging experience and resolving common issues (now, the only local tool is IT Forum (Bitola));
4. Definition and establishment of clear ICT hierarchy within judiciary, responsibility and area of competence at every level, creating efficient communication processes (new organization);
5. Centralized, long-term planning of all ICT needs;
6. Ensure minimum annual, compulsory ICT (certified) training for all ICT staff;

7. Justice ICT organization structure – to be clearly established, according to the best efficiency principle.

We think it is important to take these proposals into consideration, when recommending solutions for the "Data Protection, Information Security and Access Rights", using them to achieve the best possible effects.

2. Elements of Information Security Policy

2.1 Purpose

Institutions create ISPs for a variety of reasons:

- To establish a general approach to information security
- To detect and forestall the compromise of information security such as misuse of data, networks, computer systems and applications.
- To protect the reputation of the organization with respect to its ethical and legal responsibilities; in case of the justice sector, and particularly courts, this is of utmost significance.
- To observe the rights of the justice system clients, citizens, non-citizens and business entities; providing effective mechanisms for responding to complaints and queries concerning real or perceived non-compliances with the policy is one way to achieve this objective.

2.2 Scope

ISP should address all data, programs, systems, facilities, other tech infrastructure, users of technology and third parties in a given organization, without exception.

2.3 Information security objectives

An organization that strive to compose a working ISP needs to have well-defined objectives concerning security and strategy on which management have reached an agreement. Any existing dissonances in this context may render the information security policy project dysfunctional. The most important thing that a security professional should remember is that his knowing the security management practices would allow him to incorporate them into the documents he is entrusted to draft, and that is a guarantee for completeness, quality and workability.
Simplification of policy language is one thing that may smooth away the differences and guarantee consensus among management staff. Consequently, ambiguous expressions are to be avoided. Beware also of the correct meaning of terms or common words. Ideally, the policy should be briefly formulated to the point.
Redundancy of the policy's wording (e.g., pointless repetition in writing) should be avoided as well as ICT would make documents long-winded and out of sync, with illegibility that encumbers evolution. In the end, tons of details may impede the complete compliance at the policy level.

Thus, how management views ICT security seems to be one of the first steps when a person intends to enforce new rules in this department. Furthermore, a security professional should make sure that the ISP has an equal institutional gravity as other policies enacted within the corporation. In cases where an organization has sizeable structure, policies may differ and therefore be segregated in order to define the dealings in the intended subset of this organization. Information security is deemed to safeguard three main objectives:

- Confidentiality – data and information assets must be confined to people authorized to access and not be disclosed to others;
- Integrity – keeping the data intact, complete and accurate, and ICT systems operational;
- Availability – an objective indicating that information or system is at disposal of authorized users when needed.

2.4 Authority & Access Control Policy

Typically, a security policy has a hierarchical pattern. ICT means that inferior staff is usually bound not to share the little amount of information they have unless explicitly authorized. Conversely, a senior person in the organization may have enough authority to make a decision what data can be shared and with whom, which means that they are not tied down by the same information security policy terms. So the logic demands that ISP should address every basic position in the organization with specifications that will clarify their authoritative status.

Policy refinement takes place simultaneously with defining the administrative control, or authority in other words, people in the organization have. In essence, ICT is hierarchy-based delegation of control in which one may have authority over his own work, single institution manager (e.g. court president or court manager, if such exists) has authority over files belonging to a group he is appointed to, and the system administrator has authority solely over system files. Obviously, a user may have the “need-to-know” for a particular type of information. Therefore, data must have enough granularity attributes in order to allow the appropriate authorized access. This is the thin line of finding the delicate balance between permitting access to those who need to use the data as part of their job and denying such to unauthorized entities.

Access to company’s network and servers, whether or not in the physical sense of the word, should be via unique logins that require authentication in the form of either passwords, biometrics, ID cards, or tokens etc. Monitoring on all systems must be implemented to record logon attempts (both successful ones and failures) and exact date and time of logon and logoff.

Resource Access Logs

ICT staff shall be responsible for maintenance of the following logs for at least 60 days for each server they support:

1. System Access Logs: should contain both successful and unsuccessful log on attempts;
2. Activity Logs: activities performed by the system administrators. ACCMIS runs its own activity logs, but is increasingly vague; ACCMIS logs do not register read access to system, also do not provide specific information on data change.

Issue Item 1: *Does every court keep these logs active, and are they checked occasionally, for breach of security?*

Local Situation Assessment 1:

Courts:

While each server OS is setup so that System Access Logs are kept, sometimes their size restricts how long they can be kept on the system, especially at large courts, and when there is a large number of events to be recorded. By law, each court must have a Security Officer, who is in charge of periodic review of all logs.

Activity Logs have been found to significantly slow down system operations at courts, so not used, considering that ACCMIS keeps its own activity logs, and it is the key system at courts (one exception is that ACCMIS does not register Read access to the system)

There is a new law on the protection of personal data, aligned with EU regulations (GDPR), which further regulates some aspects of this area.

Prosecution Offices:

Situation is similar to the courts, with the difference that their Case Management System (CMS) is a more modern, centralized system, with no local installations (all users access the system through web). CMS, unlike ACCMIS, registers all types of access, including Read-only.

Action Items 1:

With the new, more powerful servers installed at all courts, all logs should be maintained.

Reporting Access Violations

1. ICT staff shall maintain a process for providing reports of invalid log-on attempts, upon request; there is no specific log tracking system in the courts, so tracking logs is almost impossible.
2. ICT staff shall maintain a process for detection and reacting to systematic attacks on the server systems that they support.

Issue Item 2: *Does every court maintain this process of providing reports on invalid log-ons, and are there any periodical requests to provide such report?*

Local Situation Assessment 2:
Courts:
According to the current regulations, Security Officer at each court must check at least twice a year adherence to the security rules, including use of logs, i.e. reports on their use. The Directorate on Data Security is authorized to conduct periodic revision of the security rules at each court, on a random basis. There is no log tracking tools or log management software at this moment, so invalid log-on attempts should be found manually, which is hard to perform and can produce incomplete reports. After the revision by the Directorate on Data Security in some courts, it was one of the remarks that emerged from this revision. Therefore, funds for the procurement of this type of software were requested several times from the Judicial Council, but funds have not been provided yet.
To make this process more efficient and comprehensive and to conduct periodic checks and reports, log tracking software is essential. The fact that Security Officers in the courts are persons that work legal stuff should also be taken into account.

Prosecution Offices:
Situation is similar to the courts.

Action Items 2:

- *Ensure that Security Officers at each court/PO regularly check all logs, in line with regulations, using new log-tracking tools*

Speaking of evolution in the previous point – as the ICT security program matures, the policy may need updating. While doing so will not necessarily be tantamount to improvement in security, ICT is nevertheless a sensible recommendation.

2.5 Classification of Data

Data can have different value. Gradations in the value index may impose separation and specific handling regimes/procedures for each kind. An information classification system therefore may

succeed to pay attention to protection of data that has significant importance for the organization, and leave out insignificant information that would otherwise overburden organization's resources. Data classification policy may arrange the entire set of information as follows:

1. High Risk Class– data protected by formal, official state legislation, as well as financial, payroll, and personnel (privacy requirements) are included here. ("High Protection Measures")
2. Confidential Class – the data in this class does not enjoy the privilege of being under the wing of law, but the data owner judges that ICT should be protected against unauthorized disclosure. ("Medium Protection Measures"). Given the nature of the work of IT people, they should also own security certificate; now only a small percentage (almost none) of IT staff have such a certificate.
3. Class Public – This information can be freely distributed. ("Basic Protection Measures").

Issue Item 3: Does this data classification look similar to the definitions in the local relevant document:
"Technical and organizational measures", as defined in Article 5 of the "Regulation for the Technical and Organizational Measures to Ensure Confidentiality and Protection of the Processing of Personal Data", issued by the Directorate for the Protection of Personal Data, in March 2009. („Правилник за изменување и дополнување на правилникот за техничките и организациските мерки за за обезбедување тајност и заштита на обработката на личните податоци")

Local Situation Assessment 3:

Courts:
In North Macedonia, there is an Institution, "Directorate for Security of Classified Information" (Дирекција за безбедност на класификовани информации, ДБКИ), which issues security certificates to all individuals requiring access to protected information, in line with the three levels of security certificates, as shown in 2.5. It appears that relatively small number of key courts staff (judges) have the highest level of certification ("High Risk Class").
At the Supreme Court, the special room for the keep of high security, secret documents is still missing, although the regulations require their existence.
ACCMIS does not have an option for handling high security cases, so these cannot be processed using this application!

Prosecution Offices:
Very small number of PO's at the Basic PO level have the security certificates, except for the Organized Criminal department; this creates a problem when a potential case appears with some classified evidence items.
CMS application does not have an option for handling high security cases, so these cannot be processed using this application!

Action Items 3:

- Ensure that sufficient numbers of judges and PO's have security certificates, including the high-level ones, in line with regulations
- Request both key applications at courts and PO's (ACCMIS and CMS) to include processing of cases with high-security certificates

Data owners should determine both the data classification and the exact measures a data custodian needs to take to preserve the integrity in accordance to that level.

2.6 Data Support & Operations

In this part we could find clauses that stipulate:

- The regulation of general system mechanisms responsible for data protection
- Systems containing personal and/or business entities information, such as those in the justice sector, must be protected in alignment with any existing national or organization or sectorial standards and sectorial best practice (if any). Such systems must operate:
    - Up-to-date anti-malware protection
    - Firewall
    - Encryption
    - Be adequately patched, whenever the need arises

Issue Item 4: are all these measures taken for protection, in all justice institutions, especially courts?

Local Situation Assessment 4:
Courts:
All the above measures have been taken in all courts!
Prosecution Offices:
All the above measures have been taken in CMS

Action Items 4:
No action items required.

- The data backup: backups should be encrypted, in line with the industry best practices, and hosted in an area of physical security. Backup media must be stored, at all times, in one of the following:
    - Computer Centre
    - Data closet
    - Single office room, locked and available only to selected staff
    - Approved off-site media storage facility is of extreme importance; most courts only backup data without checking the functionality and consistency of the data. Firstly, because there is no unified procedure for checking the returned data, and secondly, because there is no real technical resources for it to be implemented.

Issue Item 5: Since it is known that the Supreme Court performs periodically these data backups, are they encrypted, and in line with the best industry practices?

Local Situation Assessment 5:

Courts:
Data backups are stored on tapes in some courts, but not all. The backups, including tapes, are stored in the server room, under key, with access only to authorized personnel. ACCMIS backups at the courts are kept on the second partition of the same single server!
Supreme Court does both incremental and full backups from all courts, using AVAMAR system for collecting backups from remote locations (courts)
It is important to emphasize that so far no procedure has been defined for data recovery and no institution is currently responsible for data recovery and system testing after performed data recovery.

Prosecution Offices:
Since PO uses CMS as centrally based system, backups are needed only at the central site; full backup is done on a monthly basis, with incremental backups done daily. However, all backups are kept on the system, without transfer to tapes. There are no clear regulations yet on this matter!

Action Items 5:

- Both courts and PO's should ensure that backups are taken regularly, according to regulations, transferred to tapes, and these kept in secure, separate locations, away from the server room

- Movement of data:
    - data transfers can be made only by secure transfer mechanisms
    - Any information on a portable device (laptop, USB, disk, etc.) to be transferred out of organization, or across public network, must be encrypted in line with commonly accepted industry standards and applicable laws and regulations (if any)

Issue Item 6: Are these rules for the movement of data respected in all institutions?

Local Situation Assessment 6:
Courts:
There is no strict control of external devices being used to copy data, such as USB, at remote sites (local courts with ACCMIS), although there are rules on this matter!
There is existing policy for USB restriction and other security policies, applied in accordance with the data protection law. There are also (in some courts) ISO procedures for: back-up management, rules for access the server room, classified information etc.
Prosecution Offices:
Since PO uses CMS as centrally based system, it is only the central site that has the data, thus it is easier to control its transfer; however, it is not strictly controlled.

Action Items 6:

- Both courts and PO's should more strictly regulate and implement policy on transfer of data to mobile devices, including encryption.

2.7 Security Awareness Sessions

Sharing ICT security policies with staff is a critical step. Making them read and sign to acknowledge a document does not necessarily mean that they are familiar with and understand the new policies. A training session would engage employees in positive attitude to information security, which will ensure that they get a notion of the procedures and mechanisms in place to protect the data, for instance, levels of confidentiality and data sensitivity issues. Awareness training should touch on a broad scope of vital topics: how to collect/use/delete data, maintain data quality, records management, confidentiality, privacy, appropriate utilization of ICT systems, correct usage social networking, etc. A small test at the end is perhaps a good idea. Information Security Awareness training key points:

- This training shall be included in the new staff introduction process
- Ongoing awareness programme, established and maintained by proper organizational part in order that staff security awareness is refreshed and updated when necessary

Issue Item 7: Are there any regular Security Awareness training sessions taking place, and if yes, who is attending? Are they organized for the new staff, at the start of their work at some of the justice institutions? Are there any standard training materials on this subject?

Local Situation Assessment 7:
Courts:
No regular, periodic specific training sessions on this subject, nor training materials; Judicial Academy does not have any such curriculum implemented. It is usually left to local ICT staff to inform other staff on security rules, when required.
Prosecution Offices:
Same situation as with the courts, with even smaller number of ICT staff in the field!

Action Items 7:

- Both courts and PO's should provide regular updates and training on security awareness, including new staff; Judicial Academy curriculum on this subject.

2.8 Responsibilities, Rights and Duties of Personnel

General considerations in this direction lean towards responsibility of persons appointed to carry out the implementation, education, incident response, user access reviews, and periodic updates of an ISP.

1. All staff shall comply with the information security procedures, including maintenance of data confidentiality and data integrity. Failure may result in disciplinary action.
2. Each member of staff is responsible for the operational security of the information systems they use.
3. Each system user will comply with the security requirements currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.
4. The above rules will be enforced at all times, provided that involved staff is properly and timely educated on currently valid ISP rules.

Issue Item 8: Is all court staff, regardless of location, being informed on the data security rules and regulations?

Local Situation Assessment 8:
Courts:
There are official procedures on this, but no official training exists, or prescribed method. It is usually left to local ICT staff to inform other staff on security rules, when required. ACCMIS has itself a problem reporting system, connected to Edusoft, support provider.
At this time, an on-site periodical control mechanism is applied by MoJ, but only at the Registry office and ICT. ACCMIS itself has built-in some controls of the case authenticity itself, but no one controls court staff whether something is printed and taken out of the court. There are no log system controls of certain documents, their access, printouts, etc.
Prosecution Offices:
Same situation as with the courts, with even smaller number of ICT staff in the field!

Action Items 8:

- Both courts and PO's should define methods for information dissemination to all their staff

2.9 Reference to Relevant Legislation in North Macedonia

(Here, all relevant national legislation in North Macedonia dealing with the information security will be listed, as well as links to any international standards, European Union and others, that are referential for the national regulations, for example GDPR)

1. "Regulation for the Technical and Organizational Measures to Ensure Confidentiality and Protection of the Processing of Personal Data", issued by the Directorate for the Protection of Personal Data, in March 2009 („ПРАВИЛНИК ЗА ТЕХНИЧКИТЕ И ОРГАНИЗАЦИСКИТЕ МЕРКИ ЗА ОБЕЗБЕДУВАЊЕ ТАЈНОСТ И ЗАШТИТА НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ„)
2. "Changes and Additions to the Regulation for the Technical and Organizational Measures to Ensure Confidentiality and Protection of the Processing of Personal Data", issued by the Directorate for the Protection of Personal Data, in December 2010 („ПРАВИЛНИК ЗА ИЗМЕНУВАЊЕ И ДОПОЛНУВАЊЕ НА ПРАВИЛНИКОТ ЗА ТЕХНИЧКИТЕ И ОРГАНИЗАЦИСКИТЕ МЕРКИ ЗА ОБЕЗБЕДУВАЊЕ ТАЈНОСТ И ЗАШТИТА НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ„)
3. "Regulation for the Standards and Rules for the Security of Information Systems used by for Electronic Communication", issued by Ministry of Information Society, June 2010

("ПРАВИЛНИК ЗА СТАНДАРДИТЕ И ПРАВИЛАТА ЗА БЕЗБЕДНОСТ НА ИНФОРМАЦИСКИТЕ СИСТЕМИ КОИ ШТО СЕ КОРИСТАТ ВО ОРГАНИТЕ ЗА КОМУНИКАЦИЈА ПО ЕЛЕКТРОНСКИ ПАТ")

4. "Court Rules of Procedure", issued by the Ministry of Justice, June 2013, Articles 12, 88 ("СУДСКИ ДЕЛОВНИК")
5. "Rules of Procedure for Amending and Supplementing the Court Rules of Procedure, July 2014" ("ДЕЛОВНИК ЗА ИЗМЕНУВАЊЕ И ДОПОЛНУВАЊЕ НА СУДСКИОТ ДЕЛОВНИК")

2.10 Other Items an ISP May Include:

Virus Protection Procedure, Intrusion Detection Procedure, Remote Work Procedure, Technical Guidelines, Audit, Employee Requirements, Consequences for Non-compliance, Disciplinary Actions, Terminated Employees, Physical Security of IT, References to Supporting Documents and so on.

Issue Item 9: are any of these additional items defined and used within the North Macedonia court systems?

Local Situation Assessment 9:
Courts:
The Supreme Court ICT staff, Judicial Council and 4 Appellate Courts are ISO-certified, with some 10 key ISO-defined procedures.
Prosecution Offices:
PO's are not ISO-certified, no additional procedures defined!

Action Items 9:

- Courts should ensure that these ISO-based procedures are regularly respected, and staff informed on them; ISO certification should also be implemented at the basic courts. PO's should attempt to get ISO-certified, same as courts!

3. Conclusion (Importance of ISP)

Out of carelessness mostly, many organizations, without giving a much thought, choose to download ICT policy samples from a website and copy/paste this ready-made material in attempt to readjust somehow their objectives and policy goals to a mould that is usually crude and has too broad-spectrum protection. Correct method is, even when one copies some ready-made ISP rules, they must be adopted to the specific needs and rules of the organization, in this case other legal rules and regulations that apply to the justice sector in North Macedonia, be it ICT for just the courts system, or other parts of the justice sector.
A high-grade ISP can make the difference between growing business and successful one. Improved efficiency, increased productivity, clarity of the objectives each entity has, understanding what ICT and data should be secured and why, identifying the type and levels of security required and defining the applicable information security best practices are enough reasons to back up this statement.

4. General Suggestions for the Justice Institutions in North Macedonia

Although there are several national documents dealing with the common information security rules for the courts listed here under article 2.9, there is a concern whether all these rules and regulations are implemented in a systematic fashion, across all institutions within the justice sector. This calls for further careful, regular inspection and assessment of these measures as stipulated here, expanding them across the complete justice system.

5. Cyber Security

Cyber security refers to security issues, procedures and methods relevant to protection of of the ICT systems and data contained within them from intrusions coming from internet. The chart underneath, from NIST (National Institute of Standards and Technology, the most well-known organization in this area), shows the accepted standard process of dealing with the cyber security threats.

This cycle of actions shows that the process starts with identifying the cyber security threats, including risk assessment, then proceeding to establishment of protection relevant to identified threats, then establishment of methods and tools for the detection of such threats, followed by pre-arranged response to these threats. After proper, pre-arranged response, the process of recovery must follow, where any damage to systems and data should be repaired. This cycle is continuously being exercised, since the threats and the risks they produce are changing with time. The issue of Cyber Security will be separately covered later.

6. Access Rights

Courts:

Regulation of the assignment of access rights is done on annual basis, using an updated document "*Raspored za rabota na sudite i sudska administracija na sudovite*". The staff from this document is then linked to the roles, as assigned by the ACCMIS system.
In this case, the "roles" are related to the different set of access rights, as defined for each specific type of work position at the court, e.g. the role of the registry clerk is different from the role of judge assistant, by assigning each one of these roles different freedom of access to various components of the system, and within them, different choice between read, write and modify rights.

Issue Item 10: How feasible and useful would be, in terms of information security, increased implementation of biometrics methods and tools in the justice sector?

Local Situation Assessment 9:
Courts:
The courts are now implementing access rights enforcement through screen usercode/password
Prosecution Offices:
PO's are using access rights to CMS as defined by the application itself.

Action Items 10:

- Courts and PO's should consider expanding their access rights methods by using biometrics and fine tuning of current access right methods

The system of assigning roles within ACCMIS seems to provide sufficient choice of various combinations of access rights, as to specifically target the work assignments for each type of the court employee, or even a specific person.
Further development of the access rights approach may require, as the technology and funding would allow, more sophisticated tools to enforce and ensure strict respect of assigned access rights. This could be done through the implementation of various biometrics tools, such as retina scan, fingerprints, and alike.

Prosecution:

The staff at the Prosecution organization is subject to the same limitations and application of rules, as pertained to their Case management System (CMS), which is a centrally installed system, as opposed to ACCMIS, which is a distributed system (one instance of the same software at each court)

7. Action Plan

This is the set of recommendations presented in the document, with further actions proposed:

ICT Council:
This document, which has already been expanded by using comments and suggestions collected from various ICT staff across the country, will be sent by our project to the ICT Council, for their further actions. We expect the ICT Council to proceed with the following actions:

a. Review the document, considering further extensions or improvements, in their next monthly meeting;
b. Assign one of the members as a rapporteur to manage the process of completing this document;
c. The ICT Council should, during its examination of this document, consider the Action Items as defined in the document, and their ramifications to the future ICT Strategy plans, as well as necessary changes to ICT Strategy, timing and financial needs;
d. Once this is done, the Council should include this document as part of the ICT strategy and send the completed document, together with proposed activities, timing and financial expectations, for further consideration to Ministry of Justice and other relevant bodies/institutions;

Action Items 1 - 10:

- *With the new, more powerful servers installed at all courts, all logs should be maintained.*
- *Ensure that Security Officers at each court/PO regularly check all logs, in line with regulations, using new log-tracking tools*

- Ensure that sufficient numbers of judges and PO's have security certificates, including the high-level ones, in line with regulations;
- Request both key applications at courts and PO's (ACCMIS and CMS) to include processing of cases with high-security certificates;
- Both courts and PO's should ensure that backups are taken regularly at all locations, according to regulations, transferred to tapes, and these kept in secure, separate locations, away from the server room;
- Both courts and PO's should more strictly regulate and implement policy on transfer of data to mobile devices, including encryption;
- Both courts and PO's should provide regular updates and training on security awareness, including new staff; Judicial Academy curriculum on this subject;
- Both courts and PO's should define methods for information dissemination to all their staff;
- Courts should ensure that these ISO-based procedures are regularly respected, and staff informed on them; ISO certification should also be implemented at the basic courts. PO's should attempt to get ISO-certified, same as courts;
- Courts and PO's should consider expanding their access rights methods by using biometrics and fine tuning of current access right methods.

Financial & Timing Ramifications:

- Changes to key courts and PO's applications (ACMIS, CMS) to include processing of cases with high-security certificates: approx. EUR 50,000, over period of 6 months.
- Selection, purchase, training and implementation of the new log-tracking tool: approx. EUR 50,000, over period of three months.
- ISO certification to be implemented at basic courts too: approx. EUR 20,000, over 4 months.
- Purchase and implementation of additional biometric tools: approx. EUR 50,000 over 6 months.

Reference List

Bayuk J. (2009). *How to Write an Information Security Policy*. Retrieved on 04/06/2014 from http://www.csoonline.com/article/2124114/strategic-planning-erm/how-to-write-an-information-security-policy.html?page=2

Entrepreneur. *Information Technology Security Policy*. Retrieved on 04/06/2014 from http://www.entrepreneur.com/formnet/form/731

IG Toolkit (2007). *NHS CFH_Corporate InfoSec Policy Template 2007*. Retrieved on 04/06/2014 from https://www.google.bg/?gfe_rd=cr&ei=kNYlU52dLOPb8gf93oG4CQ#q=NHS+CFH_Corporate+InfoSec+Policy+Template+2007

Olson, I & Abrams, M. *Information Security Policy*. Retrieved on 04/06/2014 from http://www.acsac.org/secshelf/book001/07.pdf

Perkins, J. (2013). *Information Security Policy*. Retrieved on 04/06/2014 from http://www.lse.ac.uk/intranet/LSEServices/policies/pdfs/school/infSecStaIT.pdf

Scott, A. (2013). *How to create a good information security policy*. Retrieved on 04/06/2014 fromhttp://www.computerweekly.com/feature/How-to-create-a-good-information-security-policy

Sophos Ltd. *SophosLabs Information Security Policy*.Retrieved on 04/06/2014 fromhttp://www.sophos.com/en-us/legal/sophoslabs-information-security-policy.aspx

Techopedia. *Information Security Policy*. Retrieved on 04/06/2014 from http://www.techopedia.com/definition/24838/information-security-policy

Timms, N. (2014). *Secure Networks: How to Develop an Information Security Policy*. Retrieved on 04/06/2014 from http://www.networkcomputing.com/secure-networks-how-to-develop-an-information-security-policy/a/d-id/1234642?

The University of Illinois (2014). Information Security Policy – The University of Illinois. Retrieved on 04/06/2014 from http://www.obfs.uillinois.edu/cms/one.aspx?portalId=909965&pageId=914038

University of Oxford (2012). *Information Security Policy*. Retrieved on 04/06/2014 from http://www.it.ox.ac.uk/media/global/wwwitservicesoxacuk/sectionimages/security/Information_Security_Policy_2012_07.pdf

New GDPR Law???