OFFICE AND INFORMATION SECURITY

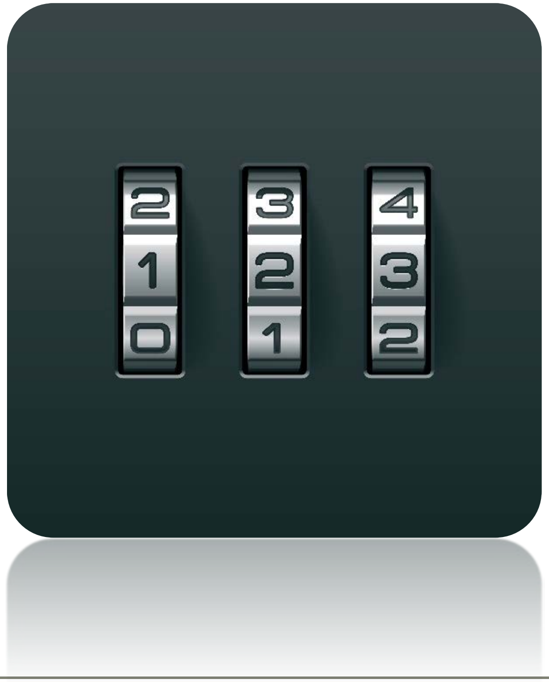
iNADO Workshop: 2016 Challenges and Opportunities in Anti-Doping

CEO Michael Ask
Anti Doping Denmark

March 13, 2016
Palais de Beaulieu, Lausanne

Agenda

- Background- the security project
- Methodology And Analysis
- The practical implementation
- Other security measures



Background

- **From interest organization to authority**
  - ADD has become subject to stricter regulatory requirements, including
  - Securing that the processing of data, documents and cases happens within the boundaries of the law, and are dealt with in a correct, proper, objective and factual manner ➔ legal protection of individuals (Public Administration Act, the Privacy Act)
- **In November 2013 we began a major review of the overall organizational as well as technical security of ADD, including:**
  - Physical access, workflows, procedures as well as IT security, etc
  - Among other things to to ensure that ADD meet the requirements for safety, under the law applicable to public authorities' treatment of personal information.
- **The Security project was initiated in cooperation with security company LinkGRC**
  - LinkGRC has extensive experience in ensuring organizational and technical security of public authorities and private organizations

Background

- **From IT Security to Information Security - one collective effort!**

- The information security policy serves as an asset that must ensure a platform of integrity and confidentiality for ADD's work with the athletes‘ data by issuing guidelines for appropriate treatment and protection of athletes' data across ADD.

- **Security is based on:**

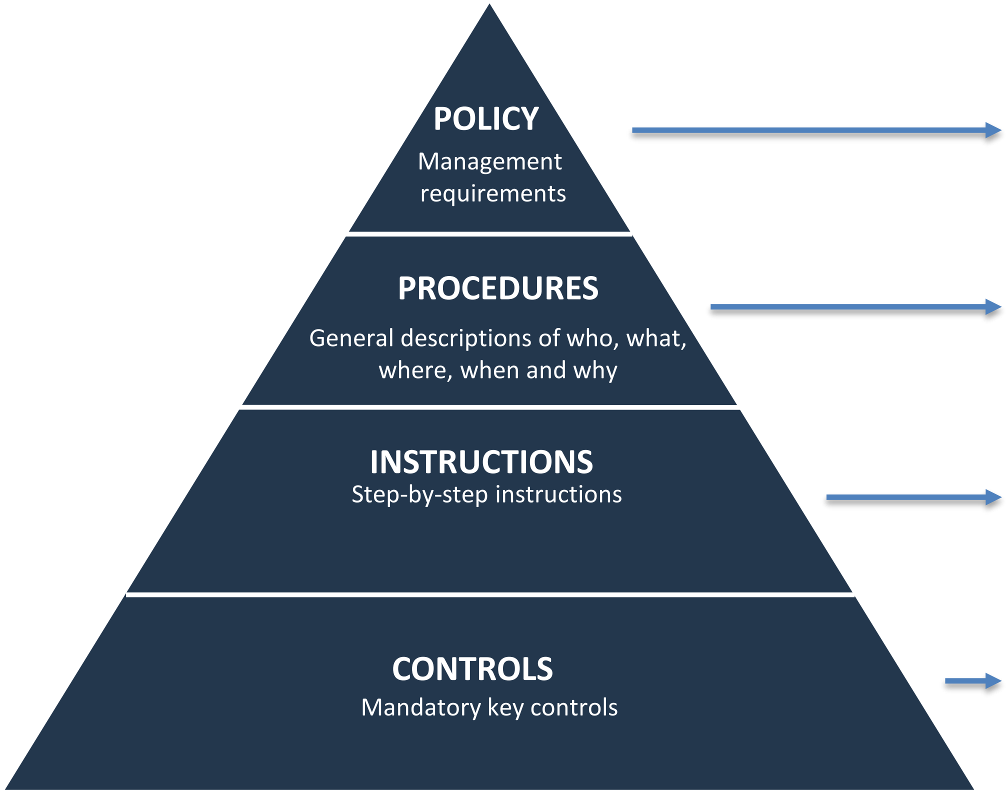
  - CONFIDENTIALITY
    - that only authorized people can access the information
  - INTEGRITY
    - that data is always reliable, ie complete, accurate and updated
  - AVAILABILITY
    - the possibility to access systems and data for authorized persons when needed

Security Objectives

- **Based on ensuring athletes procedural and fundamental rights and to comply with applicable laws, the goal is:**

- **“To have an high information security level for all employees, users and partners as well as for the use of IT resources, such as IT systems, hardware and electronic media in ADD”**

Governance framework



POLICY
Management requirements

PROCEDURES
General descriptions of who, what, where, when and why

INSTRUCTIONS
Step-by-step instructions

CONTROLS
Mandatory key controls

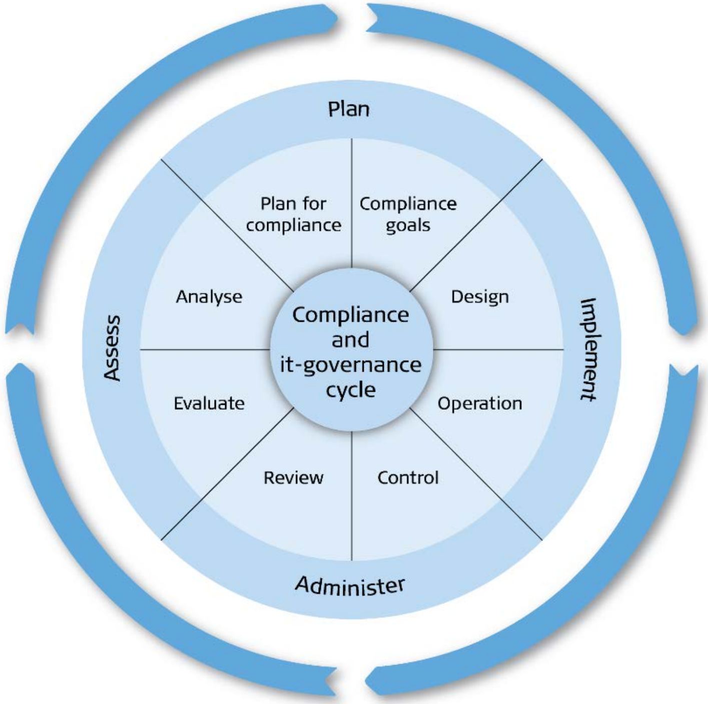
A Policy describes in clear and simple terms how the company or departments want to deliver their services to customers or business.
Policies provide principles that can help in the decision making process.
Policies must be approved by the mangement or the Board.

A Procedure is a document that supports one or more specific areas described in policies. A procedure is designed to describe the who, what, where, when and why in relation to support the implementation of a given policy area.
Procedures must be approved by management.

An instruction describes a number of steps to accomplish a task. The format is typically text, but images can also provide instructions.
Instructions must be approved by the person responsible for the affected area.

A control shall be designed so that it provides the best possible assurance that information security in the organization or the individual area are functioning properly; that the integrity of the information is intact and comply with laws, rules, standards and good practice.
Controls must be approved by management.

Cycle for Governance, Risk og Compliance



Governance framework

WHAT DO WE WANT?	Statutes for ADD	Procedures of the Board	Agreement with the Ministry of Culture and ADD Strategy for 2016-2018
WHAT DOES THE LAW SAY?	ISO27001/2:2013	The Privacy Act	National anti-doping rules
	Anti-doping Regulations for fitness centers	Act on Promotion of integrity in sport	Order on the promotion of drug-free sport
	Act on the promotion of drug-free sport	Act amending the Act on the promotion of drug-free sport	Act amending the Act on the promotion of drug-free sport
	Act to amend the Act on allocations ...	Act to amend the promotion of drug-free sport and the Tax Assessment Act	Act prohibiting certain doping substances
	Act to amend the Act prohibiting certain doping substances	Act to amend the the Penal Code	Act on distribution of profits from the lottery ...
HOW WE DO IT?	Policies	Procedures	Instructions / Guides
HOW DO WE ENSURE THAT WE DO THINGS PROPERLY?	Controls	Self assessment	Awareness

ANALYSIS

- **Identification of all ADD's assets and business processes**

- **Risk assessment of information security**
  - business systems, infrastructure, documents and data

- **Reports**
  - Summary of Information Assets, retention requirements and classification
  - Development of information security policy
  - Preparation of 17 procedures
  - Drafting of instructions and controls

ASSETS

ANTI DOPING DANMARK

ADD ANTI DOPING DANMARK

Business Systems

- ABP Database
- ADAMS
- ADRQ (WADA)
- AntiDoping APP
- COE Questionnaire
- CPRSøg
- Doping register
- Filserver
- Internet
- ADDIN (Intranet)
- Kontrol-databasen
- Kvalitetsys ADD
- Lessor Lønsystem
- Maconomy
- Office 2013
- Office 365
- Renvinder. dk
- Sitecore CMS
- SKAT. dk
- Stopdoping Etik
- Timestream

Infrastructure Systems

- Antivirus
- Applikations server
- Database server
- FTP
- VPN Software

Infrastructure components

- Bærbare
- Fax
- Firewalls
- IPADs
- Mobil telefoner
- Printere
- Routere
- Stationær
- Switch
- Telefon
- Telefon system

Documents

- Advarsels brev
- Aftaler
- Ansøgninger og CV
- Ansøgnings Skema TUE
- Bestyrelses møde materiale
- Bestyrelses møde Fortroligt
- Budgetter
- Kendelse
- Kvartals rapporter
- Notater
- Notater Følsomme
- Overdrag elsesbrev
- Protokoller Negative
- Protokoller Positive
- Regnskaber
- Risici
- Statistikker
- Strategi
- Årsplaner

Data

- Aprøver
- Bprøver
- Biologiske data
- CPRnr
- Disciplinær straf
- Kontaktdata Fortroligt
- Kontaktdata Generelt
- Løninforma tioner
- Medicin
- Regnskabs poster
- Resultater ift atlets biologiskpas
- Test chain o custody negative
- Test chain of custody positive
- Test doping kontrol formular negativ
- Test doping kontrol formular positiv
- Test mission orders negative
- Test mission orders positive
- Test resultater AT
- Test resultater negativ
- Test resultater AAF
- TUE godkendelses formular
- TUE medicinske informationer
- Whereabouts
- Whereabouts ift atlets biologiskpas

ADD’s 17 Procedures

- Access Control
- Protection of Information Assets
- Operation controls of service provider
- Physical security
- Incident management
- Information Assets
- Encryption
- Service Level Agreement
- Logging and monitoring
- Personnel security
- Personal Information
- Project, delivery and task management
- Risk management
- Managing IT security incidents
- Vulnerability Scanning
- Development and testing
- Change management

Photo:Tom Raftery

Independent IT operating environment

- **Went from an "uncertain" common IT operating environment to a 100% independent and closed IT operating environment**

That is:

- Our own SLA (service level agreement)
- Our own server environment, print server and printer, own AD (Active Directory), a private wired and wireless network, etc. in order to improve IT security as well as:
  - Improve monitoring/surveillance of access to ADD's information and data
  - Facilitate the process of setting up operating controls
  - Minimizing the risks of error when creating / disabling of users etc.

Service Level Agreement (SLA)

- **Power & Cooling**
  - Dedicated transformer
  - Own emergency power system consisting of redundant uninterruptible power supply (UPS) and 400 KVA diesel generator
  - Separate redundant cooling unit

- **Physical security**
  - Datacenter with the latest alarm technology (each employee has electronic-key and personal code)
  - The whole building is monitored internally and externally via IP cameras with motion detectors
  - Security Guard (dog patrol assigned 24 hours/day)

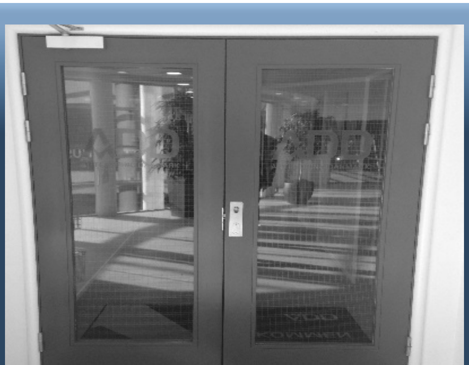
- **Fire protection**
  - The data center is equipped with inergen systems for fire-fighting (when a fire, the system will pump 220,000 liters of fire extinguishing agent (inergen) into the server room.
  - The entire building has ABDL fire alarm (automatic fire door-close systems) with direct connection to Aarhus Fire Brigade

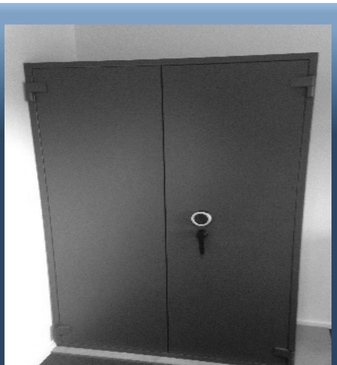
- **IT security**
  - Firewall (Cisco ASA 5500 Series Security Appliances)
  - Antispam (using. Smartermail and Microsoft Exchange spam filters)
  - Patching (continuous Windows update)
  - Antivirus (MS Forefront security antivirus scanning system and MS Intune Endpoint Protection)

PHYSICAL SECURITY

- **Mapping the current framework for physical access to ADD**
- **Developed instructions for physical access to ADD**
- **Installed new entry system** (automatic door lock and intercom)
- **Signed agreement with security vendor on the safe storage, collection and shredding of sensitive personal and other confidential information** (Danish Security Shredding)

- **Secure physical storing of particularly important and confidential documents**
  - Installed two locked fireproof document cabinets, in two different locations





Access Control

We need to know what needs to be secured, how it should be secured and who is in charge of securing it.

- There has been established a base line for access control in ADD, which has resulted in a centrally located list of systems etc. that employees of ADD and partners use in their daily work.

- Furthermore, employees' existing entries, roles etc. in the systems, has been mapped.
  - Based on this, every employee has been assigned a file with their rights to the business systems they use
    - Access Roles (rights - r / w)
    - Password policy

Operational controls

- **There has been develop a detailed operational controls plan for our IT hosting partner as part of the SLA.**

- The Operational Control plan includes monthly to annual checks that all operating requirements are met

- The plan specifies how the hosting partner must document the above mentioned.

Supplier Management

- **Developed instructions to all data processors, to ensure that they:**
  - Comply with the general rules on data security laid down in the Act on Processing of Personal Data (Privacy Act) §§ 41-42
  - Provide a statement of assurance annually or when major changes take place in the treatment of data, documenting the level of security is in place in accordance with Act on Processing of Personal Data
  - Delivers a workflow description which describes how the processor handles the data and who is authorized to do so at the processor
  - Processes personal data in accordance with best data processing practice etc. as stated in the Act on Processing of Personal Data §§ 5 -8
  - In addition, the Act on Processing of Personal Data provisions are generally applicable to all processing carried out by the signatory data processor

Personnel security

- **All of the secretariat employees at ADD are in the process of being security approved by PET (Danish Security and Intelligence Service)**
  - The first two are already approved

- **All employees has signed a confidentiality agreement.**
  - and is subject to the Criminal Code and security Circular

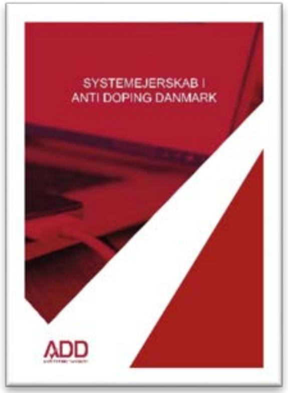
Encryption

- **Enabled encryption to secure email communication for all employees working at ADD**
  - All employees send and receive sensitive and confidential information encrypted
  - This in order to ensure data integrity and comply with the rules for handling this type of information.

AWARENESS

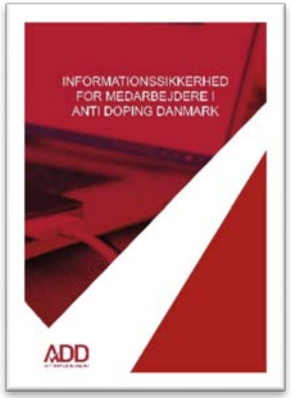
- **Organizing awareness workshops with key players in the field of security**

- **Developed various materials:**
  - “Information security for employees”
  - “System Ownership at ADD”
  - Poster with 10 tips on safe behavior



SYSTEMEJERSKAB I
ANTI DOPING DANMARK

ADD



INFORMATIONSSIKKERHED
FOR MEDARBEJDERE I
ANTI DOPING DANMARK

ADD

CSIS

FORSVARETS
EFTERRETNINGSTJENESTE

FE

ADD
ANTI DOPING DANMARK

10 TIPS ON SAFE CONDUCT

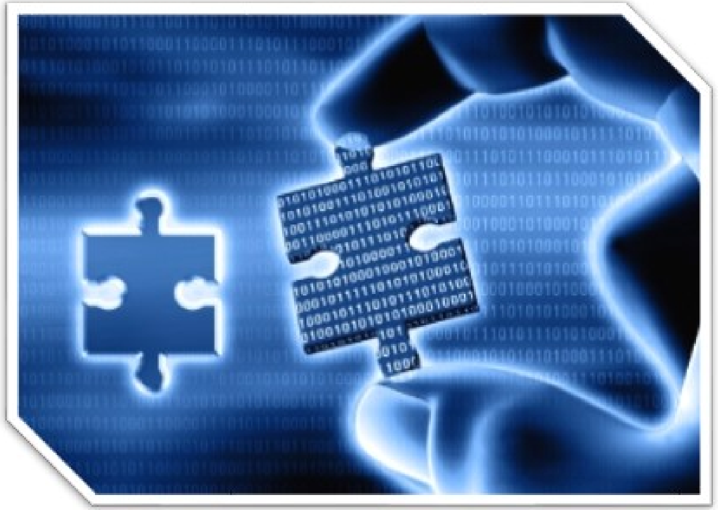
1. Make a secure password
2. Your password is personal - do not share it with others
3. Lock your PC when you leave your seat (Windows key + L)
4. Never store any data on the “desktop” - Save in ECDM
5. Always send person sensitive and confidential information through secure mail
6. Do not open e-mails where there is uncertainty about the content (attachments, strange links, desire bank information, etc.).
7. Do not download programs directly from the Internet unless you fully trust the vendor
8. Always keep your PC updated (browser, Java, Adobe Acrobat Reader DC, etc.)
9. Always shred papers with sensitive or confidential information
10. Check that doors and windows are closed when you leave

Use your common sense and ask others for help if you are in doubt!

ECDM (Electronic Case and Document Management system)

- **Safe and structured processing of the business information**

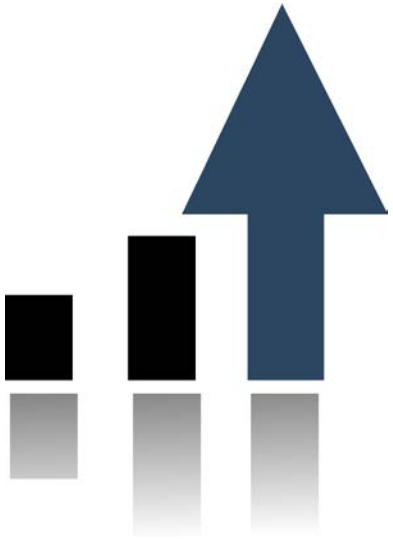
- **It is good governance:**
  - To archive documents received or sent by an authority as part of administrative proceedings relating to its business, to the extent that the document is relevant to a case or proceedings in general.
  - Having version control
  - To log all actions



Why use an Electronic Case and Document Management system

Internal advantages:

- Increased efficiency
- Better service
- Lower costs
- Better control with data
- Reduced risk
- Enhanced security
- Knowledge sharing
- Less time wasted on searching information
- Improved quality
- Effective and skilled handling of public acces to documents
- Reliable partner to other government departments that have similar systems
- Honor athletes and partners (legitimate) expectations for safe handling of data, efficient use of resources, etc.

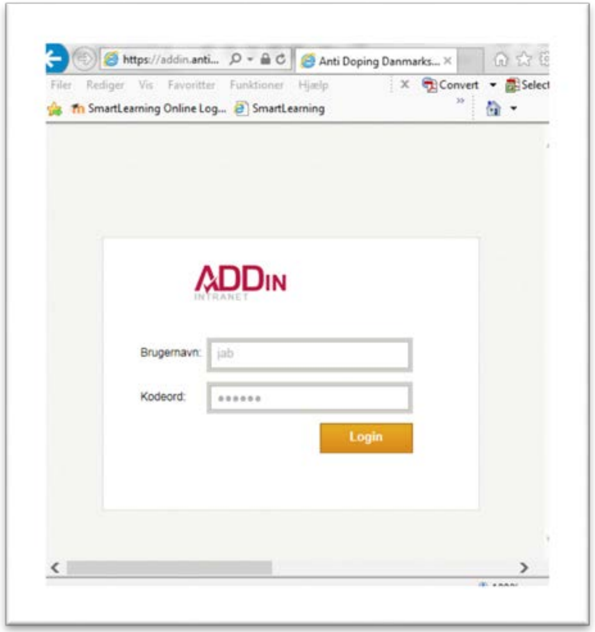


MOBILE SAFETY

- **Password**
  - 6-digit password on all mobile devices
- **Auto lock**
  - The mobile device locks after a maximum of 30 sec's inactivity
- **Find my iPhone**
  - The app "Find my iPhone" shall be enabled
  - This means that if the mobile device is lost or stolen it can be traced and all data can be deleted.

Login to the intranet (ADDin) and our Remote Desktop

- Multi-factor access
- HTTPS (SSL) – encrypted site



https://addin.anti...
Anti Doping Danmarks...
Filer Rediger Vis Favoritter Funktioner Hjælp
Convert Select
SmartLearning Online Log... SmartLearning
ADDIN INTRANET

Brugernavn: jab

Kodeord: ••••••

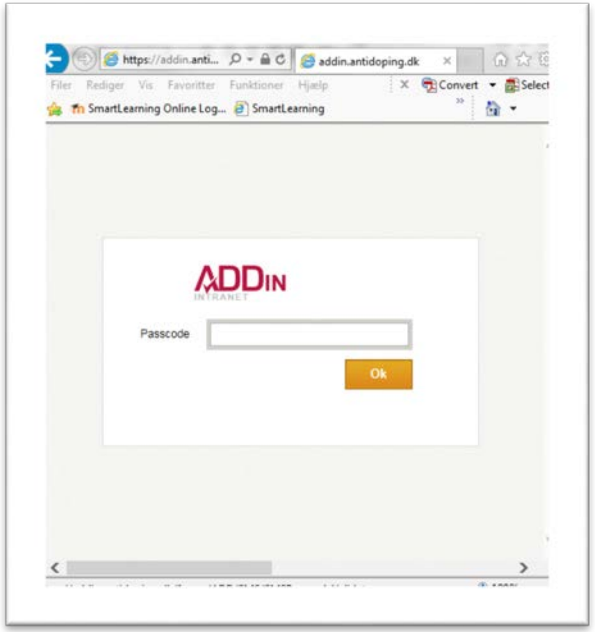
Login

+

3G 9:41 AM
“On May 19 remind me it's dad's birthday”
Here's your reminder for May 19, 2012 at 9 am:
19 Saturday
Cancel Confirm

Rodk74uu

+



https://addin.anti...
addin.antidoping.dk
Filer Rediger Vis Favoritter Funktioner Hjælp
Convert Select
SmartLearning Online Log... SmartLearning
ADDIN INTRANET

Passcode

Ok

Whistleblower Communication Center

- **Reporting is done through an encrypted and anonymous reporting form**
  - All that is recorded is the actual intelligence. Neither the computers IP address or machine ID, will be logged. Cookies are not used or stored.

- **You are also able to call anonymously to the Whistleblower hot line**
  - This is an IP voicemail, where you can anonymously leave your information without having the phone number traced.

Positive and less positive

Positive:

- Control of data, data storage and data traffic
- Reduced risk of error or deliberate manipulation of data
- Reliable partner for other public authorities that have similar systems
- Possible / easier to engage in intelligence cooperates

Less positive:

- Increased operational costs – both with respect to increased personnel - as well as financial resources
- Increased level of complexity - ie less "flexibility“
- Any operational benefits arising out of being on common network and server environment disappears.

New projects

- All employees shall be security approved by PET (Danish Security and Intelligence Service)
- Implement mobile exchange policy - centrally controlled security on mobile
- Install video monitoring of access to ADD
- Focus on IT security incidents
- Look at vulnerability scanning
- Further awareness on safe conduct for employees

Photo: Yuri Samoilov

Where are we heading ;-)?

Here at the airport we have different security measures.
Some traditional. Others brand new!
IRIS RECOGNITION
ANUS RECOGNITION
WWW.WULFFMORGENTHALER.DK

THANK YOU FOR YOUR ATTENTION!