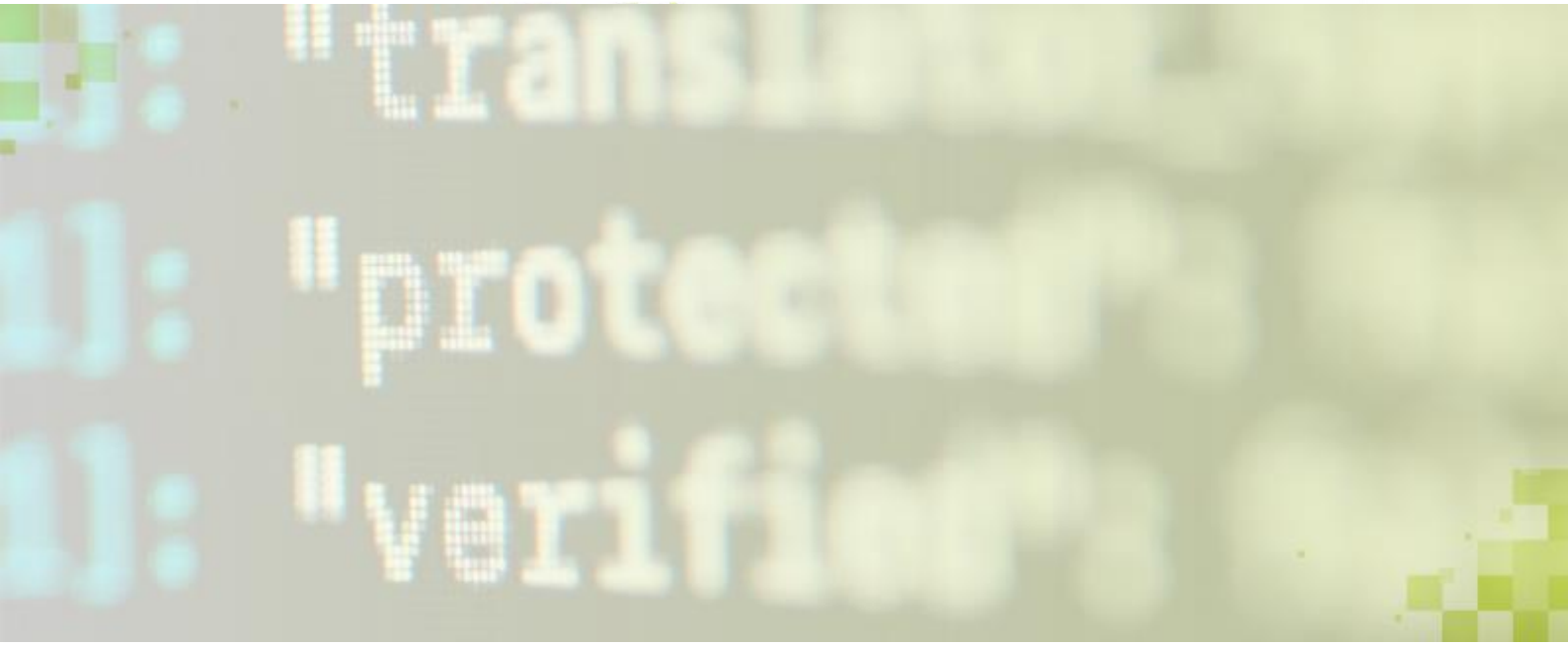

IT-security Principles for Anti-Doping Organizations

iNADO
December 2020

Heussallee 28, 53113
Bonn, Germany

IT-security Principles for Anti-Doping Organizations

Date:	December 2020
Document Name:	IT-Principles_01
Version:	1.0
Distribution:	Public/ Anti-Doping Community

The iNADO member NADOs from the following countries contributed to the development of this document:

AUSTRALIA (SIA), **NEW ZEALAND** (DFSNZ), **DENMARK** (ADD), **FRANCE** (AFLD), **UNITED KINGDOM** (UKAD), **NORWAY** (ADNO), **GERMANY** (NADA GERMANY), **USA** (USADA), **CANADA** (CCES), **SOUTH AFRICA** (SAIDS) AND **THE WORLD ANTI-DOPING AGENCY** (WADA)

*"Cyber-attacks **come in many shapes and sizes**, but the vast majority are very basic in nature, carried out by relatively unskilled individuals. They are the digital equivalent of a thief trying your front door to see if it's unlocked. **Our advice is designed to prevent these attacks**."*

- UK Cyber Essentials

TABLE OF CONTENTS

1. Introduction & Intention 3
1.1 Main objectives 3
2. Process & Resources 3
3. Threats and risks to IT-security identified 5
4. IT-principles for security compliance and improvement 8
4.1 IT-security levels 9
4.2 Identification of the level of IT-security 9
4.3 IT-security principles for ADOs 10
5. Solutions proposed 14
5.1. Roles and responsibilities for developing a security system 15
5.2. Proposal of data classification 17
6. Last words 18
7. Annex 18
7.1. ADO IT-security Questionnaire 19

1. Introduction & Intention

After a series of cyber-attacks upon a dozen NADOs in the fall of 2019, a group of iNADO members expressed the need to share experiences and best practices between iNADO members to better prepare the community for such threats in the future.

In 2020 iNADO initiated a discussion with IT-experts of our community. The goal of this group was to create a forum for Anti-Doping Organizations (ADOs) to stay updated and raise awareness about this issue in general; more specifically share experiences that could help in the identification of risks to IT-security, as well as methods and tools implemented to enhance IT-security.

As a result of the discussions, the present document was compiled designed as an on-going and easy-to-use list of IT-security principles (hereafter IT-principles) for national, regional and other ADOs to guide them in implementing and maintaining a minimum level of IT-security in their organizations. The clear and humble intention of this document is to provide user friendly, tailor-made, jump-start guidelines for the anti-doping community.

1.1 Main objectives

- Meet Strategic Goals of ADOs: Risk mitigation and asset protection.
    - Mitigate information security risk to a manageable level that is accepted by the management of the ADO.
- Provide ADO users with the highest level of IT-service.
    - Protect and prevent information (e.g., athlete personal data, medical records, etc.) from unauthorized access.
    - Ensure that information security is integrated to essential business activities.
    - Prioritize information security to protect the business application where a security incident would have the worst impact.
- Maintain compliance obligations with the World Anti-Doping Code and International Standards.

2. Process & Resources

The risks and principles listed in this document are inspired from existing IT-security frameworks and certification programs.

In no way does this document replace comprehensive IT-frameworks that come in high recommendation for more advanced users or countries for which these can be legal prerequisites for conducting their operations.

Organizations interested in implementing a more comprehensive and already established security framework can visit the following pages:

- NIST Privacy Framework [1]: National Institute of Standards and Technology of the US Department of Commerce to learn more about their privacy and cybersecurity frameworks.
- IEC[2]: International Electronical Commission publishing International Standards for all electrical, electronic, and related technologies.
- Cyber Security Essentials of the UK Government[3]: This framework serves to guide and certify small and medium size enterprises in the UK in IT-security. Further, the IT-security indicators contained are split into two levels: basic and advanced.
- ANSSI security guide[4] From the French National IT Cybersecurity Agency, this guide purposes a list of simple IT security rules. Each rule can be taken independently, and it gives proposals to increase IT security level. A version in English is also available.
- ISO/IEC270001[5]: Information Security Management. This ISO Standards family comprises of about a dozen of Standards enabling "organizations of any kind to manage the security of assets such as financial information, intellectual property, employee details or information entrusted by third parties."

Other additional resources:

- COBIT[6]: Control Objectives for Information Technologies management and IT governance. created by the Information System Audit and Control Association (ISACA) for IT good governance.

[1] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf
[2] https://www.iec.ch/
[3] https://www.ncsc.gov.uk/cyberessentials/overview
[4] French: https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf; English: https://www.ssi.gouv.fr/en/guide/40-essential-measures-for-a-healthy-network/
[5] https://www.iso.org/committee/45306/x/catalogue/p/1/u/0/w/0/d/0
[6] https://www.isaca.org/resources/cobit

- Essential 8 Scorecard[7] IT-security performance measuring tool.
- IRAP [8]: The Information Security Registered Assessors Program based on ISO 27001.
- ISM[9]: Australian Government Information Security Manual based on ISO 27001.

3. Threats and risks to IT-security identified

Before going into the details of the IT-security principles, it is worth mentioning which IT-security *threats and risks*[10] ADOs are generally exposed to and that this document will help to address. The main issues identified by the working group of NADOs and WADA are listed and defined below.

Threats and *risks* seem very similar terms, but they are different. Knowing this difference will help ADOs to understand better the scope of this document.

- **A Threat** is defined as an external or internal matter that can exploit the vulnerability of your organization (i.e. weaknesses, gaps) intentionally or accidentally.

- **A risk** comes as a result of a threat, exploiting its vulnerability and represents the potential extraction, loss, damage or destruction of the assets of your organization: people, information, property (e.g. your staff, the athletes and their support personnel or anyone else).

Risk = **Threat** x **Vulnerability**

ADOs should be aware of the threats existing in the environment they operate in, internal (often human factor/ negligence) as well as external. These are the main risks identified by the groups and that some NADOs have been already been faced with:

[7] https://www.huntsmansecurity.com/products/essential-8-security-scorecard/
[8] https://www.cyber.gov.au/acsc/view-all-content/programs/irap/what-is-irap
[9] https://www.cyber.gov.au/acsc/view-all-content/ism
[10] Definitions provided in the document were inspired from definitions given by TAG, The Threat Analysis Group: https://www.threatanalysis.com/

- **Phishing** is an approach whereby cyber-criminals access the account or data of a user or an entire organization by disguising their identity, often by pretending to be a legitimate and well-known service provider. The deceived person is requested via fallacious reasons to provide password or other type of confidential information via a fake link to the said organization.
    - Phishing was identified by many as the weakest link of IT-security as its success mainly relies on human ignorance or negligence.

- **Brute-force-attack** is an exhaustive key search run onto a system, a database, or a website by which the cyber-criminal tries different possible passwords until guessing the correct one (also known as **Password spraying**) and mainly bets on organizations using short passwords: trying many short passwords with many organizations at once. Brute-force attacks can also take the shape of **dictionary attacks** for longer and more complex passwords. In opposition, in a **blasting attack**, cyber-criminal would try to gain access to one account by trying out multiple passwords on the same account simultaneously. Brute force attacks are usually rather long to implement, and their success relies on the user's password weakness.

- **Credential stuffing** can be one of the consequences of a brute-force attack: once a username and a password have been hacked, they can be used to gain access to multiple web applications. These are made even stronger and more devastating as many users use the same passwords and username for multiple sites and platforms.

- **Malwares**[11] are softwares that are primarily designed to access and damage a system (computer server, network, database…). Malwares can exist in various forms such as *trojan horses, viruses, adware, ransomware, spyware, etc.*
    - ***Ransomware*** typically blocks access to a system until the user pays a ransom to the hacker, being the only way for them to get access back to their system.
    - ***Spywares***' function, once the user has granted them access/ installed them (e.g. via phishing), is to observe, spy, collect information on a system or a user with the aim to share the content with external entity(ies) and serve the interest of third party, to harm user and tier stakeholders (e.g. athlete confidential information, ADO staff personal files). Spyware may also be the feature of legitimate software and websites (via web tracking and confidentiality and privacy settings).

[11]Sources of definitions on Wikipedia.com

- **Website hacking** can take various forms, but consists of obtaining unauthorized access, control and/other privileges of a website (SQL injection and XSS scripts can be used by hackers to steal information).

Such threats, if not responded to adequately could translate into the following risks for ADOs:

- Loss of data (e.g. Registered Testing Pool (RTP), lists or work emails).
- Disruption in activities (e.g., no access to emails or files temporarily).
- Unauthorised access to and/or use and dissemination of (sensitive) data (e.g. Therapeutic Use Exemption (TUE) information).
- Higher operational cost and/or money extortion.
- Loss of reputation and trust.
- Loss of data integrity and increased vulnerability: higher exposure to other threats and future attacks.
- Non-compliance against the Code and the International Standard for Protection of Privacy and Personal Information (ISPPPI).

Entities wanting to or having tried to compromise organizations can be diverse, e.g.:

- Countries.
- Organized Crime.
- Lone Hacker.
- Hacktivist (someone who uses hacking methods as a means to achieve political or social change).
- Former Employees.

And with different motivations:

- Stealing information.
- Sabotage.
- Embarrassment.
- Phishing-pecuniary interest.

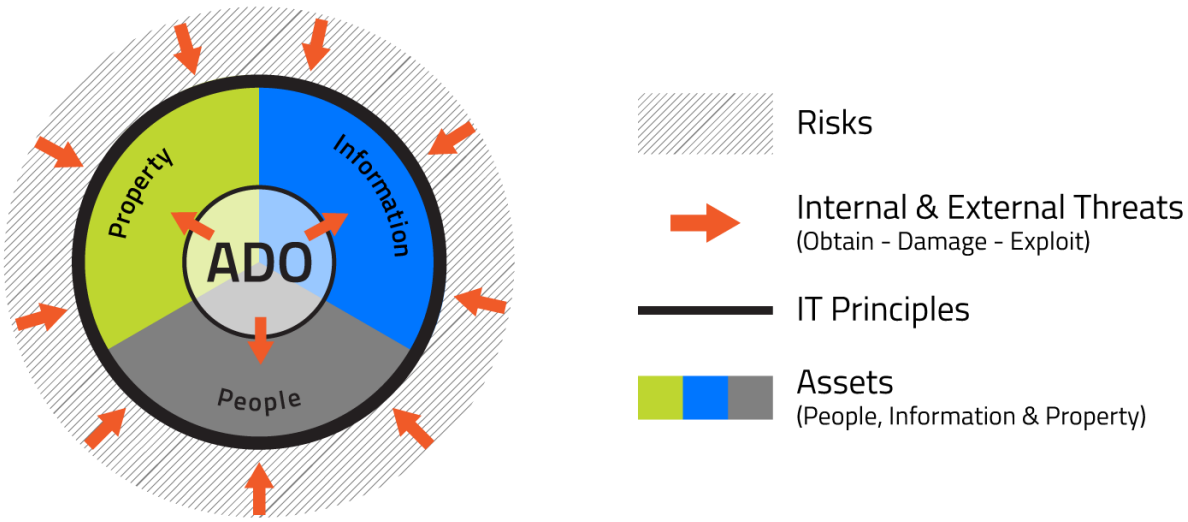

Figure 1: The aim of the principles is to mitigate these risks and remediate to IT-security incidents should they occur.

4. IT-principles for security compliance and improvement

ADOs will vary in their infrastructure, resources and in the experience of their staff in this area. Nevertheless, all are subject to the same business and legal obligations. Hence they should aim at the same security goals:

Compliance Obligation:

- National data privacy regulation
- ISPPPI

Customer and User obligations:

- Maintain trust (real and perceived)
- Protect data (personal and highly sensitive that must be kept private and secure)
- Maintain availability of the services

4.1 IT-security levels

This document has been designed with the intention to make core principles of IT-security easily digestible for ADOs of all sizes. Therefore, the principles are listed in three levels:

- ***Basic level*** is composed of requirements that all ADOs should accomplish to ensure the organization has a minimum level of IT security.
- ***Intermediate Level*** is composed of transitional principles that ADOs - having already implemented basic requirements - are encouraged to progressively implement to raise their IT-Security level.
- ***Advanced level*** contains a more comprehensive version of principles, which require additional IT-experience and infrastructure.

4.2 Identification of the IT-security level

ADOs are invited to check the maturity level of their IT-security by answering a self-assessment questionnaire (NADO Security Survey)[12]. The questionnaire was originally developed by Sport Integrity Australia to support the development of IT-security in Australian National Governing Bodies (NGBs).

The “maturity level questionnaire” in the Annex (7.1 ADO IT-security Questionnaire) of this document is based on the original self-assessment. Additional questions were added to help you assess more “business-oriented” considerations and additional elements (non-rated) that could support the decisions process for the IT-security strategy of ADOs.

The questionnaire integrates a simple and non-binding scoring system, assigning your answers to the categories mentioned before: basic/ intermediate/ advanced. Depending on your results, it is advised to start following the IT-principles applicable to your level.

[12] https://forms.microsoft.com/Pages/ResponsePage.aspx?id=pnpAsOOdm0eORvBROT8-idTXVFopuaFCk_TH17OaudZURDM0VDBMNkRFNUU3QlJXVDhBUFpZMTlLTC4u

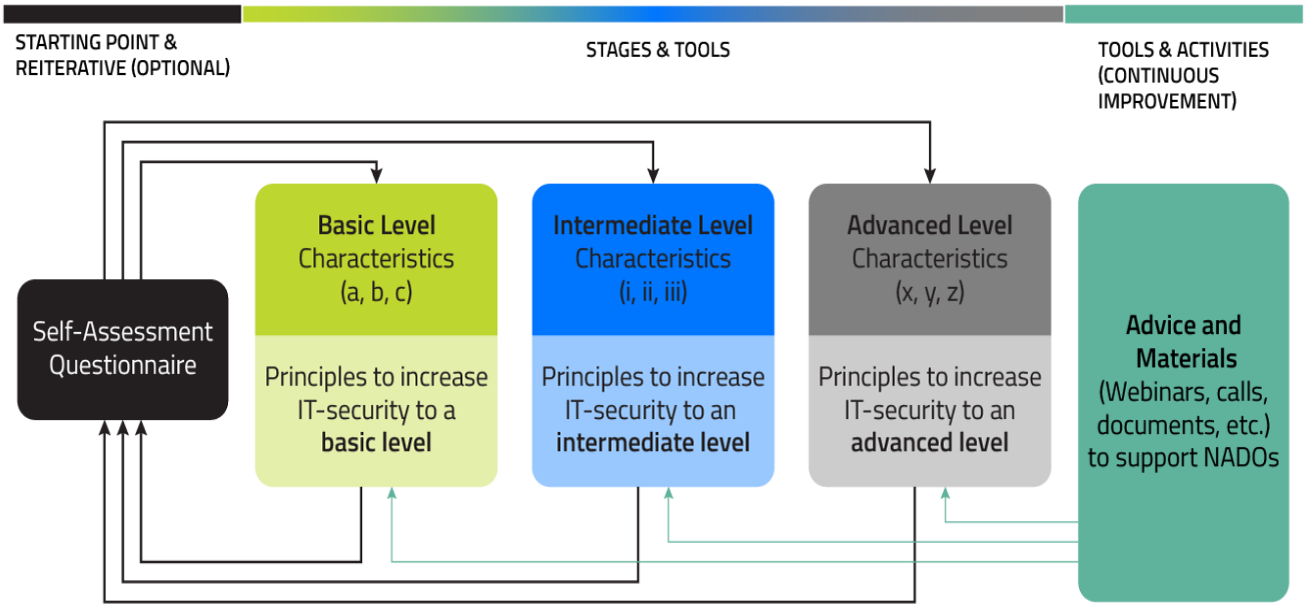

Figure 2: Process to identify and improve IT-security in your organization.

4.3 IT-security principles for ADOs

The list of IT-principles below is neither exhaustive nor do they guarantee 100% protection. Nevertheless, these IT-principles and the questionnaire should help the reader to establish the actual maturity level of their ADO and embrace a professional approach to IT-security by doing what is in their capacity to protect their information and systems.

Seven principles were identified. For each of them, at least one example is listed for a better understanding and practical application.

Basic Level	Intermediate Level	Advanced Level
1. IDENTIFY CRITICAL DATA YOUR ORGANIZATION POSSESSES AND NEEDS TO PROTECT.		
Examples listed below can be considered in ref. to "5.2. Proposal for Data Classification"		
• Organize and categorize your data in specific folder/tags. See for ref. *5.2. Data Classification*. • Identify and communicate about access authorization. • Keep a record of incident. • Keep the number of employees with administrator roles at a minimum.	• Restrict access to folder and data via a matrix (e.g.: no access, reader access, edit access). • Keep a record of security incidents, flaws, or threats. • Keep and maintain your IT network schema and locate your sensitive data servers.	• Encrypt *sensitive information* (e.g. identified as per your Data Classification. e.g. Information shared with laboratories, external committees. • Prepare communication (internal and external) scenario in case of any incident. • Keep record of sensitive data access and manipulation (edition, suppression…).
2. ASSIGN SOMEONE IN YOUR ORGANIZATION WITH IT RESPONSIBILITY.		
Examples listed below can be considered in ref. to "5.1. Roles and responsibilities for developing a security system"		
• Have one or more persons working with IT. • Keep the number of employees with "Administrator role" at a minimum.	• Have one or more persons working with IT and Security. • Keep and maintain an inventory of all 'super' accounts.	• Have one or more persons working with IT, Security and Quality (i.e. GDPR[13], ISO 27001, etc.).
3. RAISE AWARENESS OF IT THREATS WITHIN YOUR ORGANIZATION.		
• Inform/ remind staff about basic IT-security concept and principles, at a minimum at the start and as a refresher on a regular basis, via staff meetings, newsletters etc. (e.g. this document and especially 3. "Threats and risks to IT-security identified" and 5.2 Proposal of Data Classification).	• Inform/ remind staff about basic IT-security through e-learning, courses, etc. • Clearly communicate about emergency next steps in case of incidents (e.g. who to contact).	• Train users as per their assigned roles, responsibilities, and the level of information they have access to. • Ensure the necessary attention of Executive and upper management to IT-security, e.g. via annual update using results of the questionnaire.

[13] European General Data Protection Regulation (https://gdpr-info.eu/)

• Clearly communicate about emergency next steps in case of incident, e.g. who to contact?		• Invite external experts to discuss/ train staff/ organization about security.
4. CONTROL THE ACCESS TO DATA.		
• Control physical access to information. • Do not allow unvetted, unauthorized people in your office. • Do not use the same passwords for different websites and tools. • Create complex and long passwords. • Place sensitive data under "restricted access folders."	• Review access permissions periodically. • Create and circulate a password policy. • Use a password manager. • Change passwords on a regular basis. • Restrict access to sensitive data only to onsite working. • Have an up-to-date entry/departure employee policy (incl. user move) that clearly defines user account access rights.	• Require prior identification and registration of people before entering your premises. • Carry out penetration tests. • Carry out unauthenticated security tests/scans. • Allow access to internal data from an external network only through VPN.
5. SECURE YOUR INTERNET CONNECTION AND COMMUNICATION TOOLS.		
• Use a Firewall. • Use protected Wi-Fi in the office. • Have "No public Wi-Fi" Policy. • Consider outsourcing servers and hosting to an external data-center or into the cloud.	• Web-access and firewall ports should be either monitored or closed. • Have a dedicated guest Wi-Fi. • Restrict the access to certain webpages/ sites when connecting via the organization network. • Use security software (DNS - *Domain Name System* - filtering).	• Limit the access of some webpages and social media. • Only allow remote access through a VPN connection. • Use SPF[14], DMARC[15] and DKIM[16] to protect your ADO against email spoofing. • Use access monitoring tools.
6. SECURE YOUR DEVICES AND SOFTWARE AND KEEP THEM UP TO DATE.		

[14] SPF: Sender Policy Framework
[15] DMARC: Domain-based Message Authentication, Reporting and Conformance
[16] DKMI: DomainKeys Identified Mail

• Use tools against spam, viruses and malware. • Enable automatic update of operating system and software. • Update hardware and software on a regular basis, as a minimum when being asked to via push-notifications. • Use two-factor-authentication.	• Use automatic update of third-party application. • Use two-factor authentication to connect sensitive applications (mailing system, professional ADO applications). • Critical patches must be applied on a regular basis. • Data stored on the devices must be encrypted. Encryption keys must be stored in IT safe place.	• Device Management for organization's devices and applications. Regular virus and malware detection. • Only use organization's devices (no BYOD *"Bring Your Own Device*" approach).
7. KEEP YOUR KNOWLEDGE UPDATED AND USE EXTERNAL ADVICE.		
• Information sharing with government bodies, NGBs, or national sport bodies on IT-security.	• Write and implement a Security Policy. • Subscribe to IT-security bulletins and newsletters. • Have an IT-security audit conducted. • Meet with IT-security experts (National Agency or governments).	• Collaborate with government bodies, NGBs, national sport bodies and national (cyber). security agencies on IT-security. • Monitor compliance with the policies. • Review, evaluate, monitor and update the organization cyber-attack response. • Monitor and evaluate technology or data related compliance risks.

Here are a few suggestions on how to work with these principles:

- **Start with the easy ones**, don't make it too complicated!
- **For basic principles, basic knowledge** is sufficient: involve all staff of your organization!
- **Raise awareness early and never stop repeating**; being self-aware of the use and the management of the IT-tools is the biggest step.
- **Work with one principle at a time**: better slow with steady progress than a quick fix.
- **Continuous improvement**: evaluate after some time and make changes if necessary. If your IT-service it outsourced, talk to your IT-provider to which solutions have been implemented.

5. Solutions proposed

Some tools/methods are proposed below to help your organization minimize threats to data and IT-infrastructure but also strengthen processes for better IT-security.

- e.g. for Principles 1, 2: **Raise general and IT-staff awareness via training**:
  - Proofpoint Security Awareness Training[17]
  - OneTrust Awareness Training[18]
- e.g. for Principle 3: **Use different levels of security** according to seniority level based on the data classification you opted for (highest security for senior management/top secret level).
- e.g. for Principle 4: **Monitoring and limitation of access** to webpages, applications and firewall ports. In general, web-access, and firewall ports can either be monitored or closed.
  - Several ADOs use Microsoft Advanced Threat Protection.
  - For encryption, members suggest Citrix ShareFile as a safe tool.
  - Your organization may even consider moving away from sending sensitive documents through emails.
- e.g. for Principle 5: **Use log aggregator tools**. A log aggregation tool aims at collecting and aggregating logs from different sources (systems logs, server logs, firewall logs, etc.) in a single centralized location and is displayed on a visual dashboard. This enables for a better analysis, management and optimized search of data, automatization of parsing tagging and filtering[19]. These tools can be as useful as to identify intrusion attempts, password sprays and network abnormalities.
  - AlienVault[20] (note: AlienVault is now AT&T Cybersecurity).
- e.g. for Principle 6: Use of Password Management Software. This is “essentially an encrypted digital vault” that stores secure password login information you use to access apps and accounts on your mobile device, websites and other services. In addition to keep your identity, credentials and sensitive data safe, a Password Management Software should have a password generator to create strong, unique passwords and ensure that a user is not using the same password in multiple places. The usage of a vault via an enterprise account is also suggested as well as avoiding the “personal” account. For instance, this will make it easier for

[17] https://www.proofpoint.com/us/resources/data-sheets/security-awareness-training-summary
[18] https://www.onetrust.com/awareness-training/
[19] Definitions inspired: https://blog.logsign.com/ and https://www.scalyr.com/blog
[20] https://cybersecurity.att.com/

instance, when an employee quits an organization, to recall, deactivate or delete all their passwords related to their work within the organization.

- LastPass[21]

- e.g. for Principle 7: **3rd party solution**: The solution should be as integrated and user-friendly as possible. Choose a solution that also proposes an **Automatic Remediation Solution**, so it can start acting as soon as an issue is detected and you do not need to wait for human intervention (e.g. breach into mailbox should automatically generate a remediation).
  - EDR **Solution** (End Point Detection and Response Solutions) is a centralized technology that supports organizations in monitoring and protecting entry points, mitigates threats and responds in an automatic way to incidents via predefined possible actions.

5.1. Roles and responsibilities for developing a security system

In line with Principle 2 “Assign someone in your organization with IT responsibility”, roles and responsibilities that an ADO could use and adapt to the level of IT-security the organization aims for are listed below.

- **Protect information assets**
  - Adhere to privacy legislation.
  - Implement security controls and solutions according to security governance requirements such as:
    - Auditing
    - Development of policies and procedures
- **Approve security policies**
  - Communicate business obligations and goals to support individuals developing policies.
- **Identify risks associated with protecting information assets and maintain a risk register**
  - Set a risk tolerance level that protects information assets and enables business operations to run as smoothly as possible.
  - Conduct threat and risk assessments as much as necessary and review the results.
  - Track and record information security risks, detailing if the risk is accepted, not accepted, mitigated, or transferred.
- **Design security systems to protect IT infrastructure proactively**

[21] https://www.lastpass.com/

  - Assess IT environment for vulnerabilities and work to close them to improve organization's information security posture.
- **Design security systems to remediate exploited vulnerabilities**
  - Incident response effort by designing solutions to security vulnerabilities used by attackers.
- **Develop information security policies**
  - Gain an understanding of the functional requirements necessary for each security policy.
  - Collaborate with individuals across departments.
  - Review compliance requirements for security policies and update annually.
  - Ensure that policies capture the current and developing security controls.
- **Maintain and ensure execution of security operational standards, such as:**
  - System hardening
  - Patching
  - Provisioning and de-provisioning of systems and access
  - De-commissioning of technical assets
  - Manage security devices (internal & external): configure, update, and tune.
- **Know what is happening in the environment: real-time security monitoring/detection**
  - Monitor the organization's IT systems and end users' activities from an information security perspective.
  - Correlate and analyze logs to detect potential information security breaches, and perform other activities needed to support the threat intelligence program.
- **Know what actions need to be taken:**
  - Security incident management
  - Security problem management
  - Reporting
  - Auditing response
  - Forensics
- **Deploy and maintain proactive security measures, such as:**
  - Anti-virus
  - Firewalls
  - Encryption
- **Conduct penetration and security awareness testing**
  - Test the strength of organization's security via common attack techniques.

- Test end-user awareness through mock phishing emails and other appropriate techniques.

5.2. Proposal of data classification

In reference to Principle 1 “Identify critical data your organization possesses and needs to protect, organizations handle a broad range of data. This is an example of data classification you may use and/or adapt to your needs:

Top Secret: Highly critical and confidential data that requires the highest levels of security. This is characterized as data where a compromise, theft, or loss would create business disruptions and affect competitiveness.

- Financial data
- Human Resources data
- Athlete/ Testing data
- Legal data
- Confidential IT data
- Regulated data

Confidential: Very sensitive data that should be protected to a high degree. Although having no single or direct ability to jeopardize the organization, this data can still have a serious business impact.

- Email containing confidential data
- Intellectual property
- Security data
- Management data
- Business strategy

Private: This is data considered to be sensitive in nature and requires at least minimal security controls to protect its Confidentiality, Integrity, Availability.

- Project reporting data
- Organizational structure
- Email containing private data
- Policy / process data

Public: Publicly available data that would not harm the organization if compromised through theft, leakage, or alteration. This level is data that needs to be secured, but if compromised, stolen, or lost, would not create major operational or viability impact.

6. Last words

The iNADO IT-security Group and WADA will continue to share materials (documents, summaries, webinars, and/or calls) to support ADOs with the interpretation and implementation of such principles.

Any feedback on this document is welcomed at: info@inado.org.

7. Annex

You will find in the following page the ADO IT-security questionnaire (based on survey from Sport Integrity Australia), developed for you to evaluate your level of security (basic/ intermediate/ advanced).

7.1. ADO IT-security Questionnaire

	Questions *(Reference to the IT-Principle the question may apply)*	**Your answers "x"**	**Your Score** *Report below the points corresponding to your answers*	
I.	**Organization User and IT-Staff**			
1	**What percentage of your organization's employees work remotely? (mobile or fixed outside of the main physical locations)**			
	ref. to: IT-Principles 1, 3, 4			
	<20%		0	
	20% - 40%		1	
	40% - 60%		1	
	60% - 80%		2	
	>80%		2	
2	**What percentage of your organization's employees have access to private or confidential data?**			
	ref. to principles 1, 4			
	<20%		n/a	
	20% - 40%		n/a	
	40% - 60%		n/a	
	60% - 80%		n/a	
	>80%		n/a	
3	**Do non-IT employees have a culture that places importance on awareness and proactivity toward security?**			
	ref. to principles 3			
	Not at all		2	
	Somewhat		1	
	Very Much		0	
4	**Do you have staff dedicated to different IT-tasks?**			
	ref. to principle 2			
	o None of the above		2	
	o IT-tasks are outsourced		1	
	o A dedicated person(s) for IT		1	
	o A dedicated person(s) for Privacy		1	
	o A dedicated person(s) for IT-security		0	

II.	IT Requirements & Compliance			
5	**Does your organization have legal regulatory compliance requirements related to confidentiality and privacy (i.e. HIPAA, GDPR, etc.)?**			
	ref. to principle 7			
	No		2	
	Minimal		1	
	Yes		0	
6	**Does your organization adhere to an IT protocol or security framework?**			
	ref. to principle 7			
	o No		2	
	o Information Security Manual (ISM)		1	
	o COBIT		1	
	o ITIL		1	
	o ISO/IEC 27000		0	
	o Other		1	
7	**Select the processes and/or policies your organization has implemented to mitigate risks and respond to incidents:**			
	ref. to principle 7			
	o None of the below		2	
	o None of the below but plan on developing in next 12 months		2	
	o Incident response plan		1: if only this answer is selected 0: if two answers or more are selected	
	o Information security policy or plan		1: if only this answer is selected 0: if two answers or more are selected	
	o Business continuity and disaster recovery plans		1: if only this answer is selected 0: if two answers or more are selected	
	o Information security strategy		1: if only this answer is selected 0: if two answers or	

			more are selected	
	o Other governance documents		1: if only this answer is selected 0: if two answers or more are selected	
8	**How do you stay up to date on IT-security? (Several options possible)?**			
	ref. to principles 5, 7			
	o Ad-hoc		2	
	o In person training		0	
	o Rely on a service provider or consultant		0	
	o Internet sources		1	
	o Media		1	
	o Edx or similar online courses		1	
	o Books		1	
	o Other		2	
III.	**Data**			
9	**How confident are you in your capacity to protect athlete information?**			
	ref. to principle 1			
	o 1 (no confidence)		2	
	o 2 (little confident)		2	
	o 3 (somewhat confident)		1	
	o 4 (confident)		1	
	o 5 (very confident)		0	
10	**Do you inform in writing your providers/end-users (e.g. laboratories) with which of your staff they are authorized to share confidential and/or private information?**			
	ref. to principles 4, 5			
	Not at all		2	
	Somewhat		1	
	Very Much		0	
11	**What percentage of your organization's data is considered to be confidential?**			
	ref. to principle 1			
	<20%		N/A	
	20% – 40%		N/A	
	40% - 60%		N/A	
	60% - 80%		N/A	
	>80%		N/A	

IV.	**Complexity of Technology Environment**			
12	**Does your organization have two or more data centers?**			
	ref. to principles 2, 5, 6			
	No		N/A	
	Yes		N/A	
13	**Do people use personal devices to access corporate systems and data?**			
	ref. to principles 3, 5, 6			
	No		N/A	
	Yes		N/A	
V.	**Business Security Requirement**			
14	**How would you rate your level of documented IT-processes?**			
	ref. to principles 5, 6, 7			
	o Basic - Undocumented and dynamic change processes.		2	
	o Repeatable - Some processes are repeated.		2	
	o Fixed - A set of defined and documented standard processes.		1	
	o Managed - benchmarked processes, effective management controls and adaptation without losing quality.		1	
	o Optimized - focus is on continuous improvement and optimization.		0	
15	**Do information security risks get marginalized or neglected in favor of end-user ease of use?**			
	ref. to principle 3			
	Not at all		0	
	Somewhat		1	
	Very Much		2	
16	**What is your organization's information security risk tolerance level?**			
	ref. to principles 3, 5, 6			
	Low risk tolerance		0	
	Medium risk tolerance		1	
	High risk tolerance		2	
17	**In the past 12 Months, has your organization suffered a security incident?**			
	ref. to principles 2, 5, 6			
	o No incidents		N/A	
	o Information not available		N/A	
	o Compromise of an email or system account		N/A	

	o Loss or unauthorized modification of data		N/A	
	o Ransomware or other malware infection		N/A	
	o Hacker attacks		N/A	
	o Successful exploitation of a phishing email		N/A	
	o Unauthorized system modification by a trusted user		N/A	
	o Phishing or other attack via a compromised partner agency		N/A	
	o Other		N/A	
18	**Do you have an active Cyber Security plan/ program/ strategy?**			
	ref. to principles 3, 5, 6, 7			
	o No		2	
	o Partly/ in progress		1	
	o Yes		0	
19	**Is security and privacy discussed regularly at the Management/ Board Level?**			
	ref. to principle 3			
	o No		2	
	o Sometimes		1	
	o Yes		0	
20	**How often is information security and privacy reported to the Management and/or Board?**			
	ref. to principle 3			
	o Never		2	
	o Ad-hoc based on requests for information		2	
	o Annually		1	
	o Quarterly		1	
	o Monthly		0	
	o Weekly		0	
21	**What would help you to improve the IT-security level of your organization?**			
	ref. to principle 7			
	o Board Awareness		N/A	
	o Increased funding or Government services		N/A	
	o Staff education programs		N/A	
	o Conferences on security and privacy		N/A	
	o Threat alerts		N/A	
	o Guidelines and advice		N/A	
	o Other		N/A	

Basic Level	Your score
21-30	
Intermediate Level	
11-20	
Advanced Level	
0-10	

- END OF DOCUMENT -