Institute of Biostatistics and Analyses

INFORMATION SECURITY POLICY
POLITIKA BEZPEČNOSTI INFORMACÍ

Issued / vydáno dne:	**2019-03-25**
Written by / vypracoval:	**Ing. Petr Brabec, Ph.D.**
Revised by / revidoval:	**Mgr. Michaela Škrabalová**
Approved by / schválil:	**Ing. Petr Brabec, Ph.D.**

Version/verze:	**QA.02.19.04**
Supersedes/nahrazuje:	**QA.02.17.03**
Valid from / platné od:	**2019-04-01**
Document length / počet stran:	**30**

Petr Brabec

Digitálně podepsal Petr Brabec
Datum: 2019.03.25 12:44:18 +01'00'

Signature / elektronický podpis

Registered e-document

History

Version	Supersedes	Changes	Valid from	Revised by
A02, rev.1	None	-	29.02.2008	-
A02, rev.2	A02, rev.1	-Update of the document base of ISMS. implementation	01.04.2009	P. Brabec
A02, rev.3	A02, rev.2	-Goals for the years 2013/2014 were updated and list of related documents was added	13.08.2013	P. Brabec
A02, rev.4	A02, rev.3	-Link to DP26 was added	19.08.2013	P. Brabec
A02, rev.5	A02, rev.4	-Goals for the year 2014 were updated	3.02.2014	R. Šmíd
A02, rev.6	A02, rev.5	-Goals for the years 2015-2016 were updated -New workplace Netroufalky was added, --Update of the version of standard - Risk owner was defined	7.02.2015	D. Klimeš
QA.02.15.01	A02, rev.6	-Revision of SOP in new template -Translation into English -Spin-off was added, chapter 1 -Links to other documents according to the update was added, chapter 4.3	30.06.2015	R. Šmíd
QA.02.16.02	QA.02.15.01	- This document builds on a shared document of the Institute of Biostatistics and Analyses MU and the Institute of Biostatistics and Analyses Ltd. (Spin-off) - see history above. -Workplace Kotlářská was replaced by Poštovská, chapter 1.1	18.08.2016	D. Schwarz
QA.02.17.03	QA.02.16.02	-Document revision in new template -The goals for year 2017 were added -The SLA was removed – this kind of contract is not used -The responsibility for initial training ISMS Policy was added -SOP.32 The intellectual property at MU was removed -P04 Plan for service improvement was added	22.05.2017	M. Škrabalová

QA.02.19.04	QA.02.17.03	- Strategic objectives were updated - Old short-term objectives were removed - Head for IT development was replaced by CIO position - The responsibilities were updated - The list of related documents was updated	01.04.2019	M. Škrabalová

Contents

Obsah

1. General Information

Management of the **Institute of Biostatistics and Analyses, Ltd.** (hereinafter referred to also as „**IBA**") considers information security management an integral part of the overall management of the activities, and includes information security into its everyday life.

At the IBA, the information security management system (hereinafter referred to as „**ISMS**") is built in full compliance with the conclusive requirements of the current version of standard ČSN ISO/IEC 27001 standard.

Information Security Policy is the basic security document of the ISMS and is binding for all IBA employees and other stakeholders obligated to ensure security by the respective agreement. Every new employee is familiar with ISMS policy immediately after his/her entry into employment. The quality manager is responsible for this familiarization.

1.1. Scope

The IBA implements the **ISMS to the full extent** of conclusive **requirements** and in line with all the principles stated in the current version of **ČSN ISO/IEC 27001** standard.

The **ISMS has been implemented, maintained and continuously improved within the entire organizational structure of the IBA** whose working site occurs in at the following address:

Poštovská 3, Brno, 602 00 and within the entire range of its activities, particularly including:

- Complete organization and management of scientific projects (registers, NIS, clinical evaluation)
- Data management
- Data analysis and results interpretation
- Software development with respect on client's requirements
- Education activities
- ICT management.

At the IBA, the ISMS is built as an appropriate part of the already established integrated management system (IMS): quality management system (QMS) and IT services management (ITSM).

1.2. Purpose and Objective

1.2.1. Standard Text Subject and Purpose of the Policy

Information security policy of the IBA represents a summary of decisions of the IBA management that determine how the defined information and other relevant assets should be protected.

This policy:

- **defines** the basic principles for ensuring a minimum standard of information security (fulfilment of the conclusive requirements of the current version of ČSN ISO/IEC 27001 standard under conditions of the respective workplace);
- **determines** the main directions and tasks through which the specified requirements should be observed;
- **establishes** frameworks of responsibilities and powers for the realization of the goals in the field of information security;
- **expresses** a clear and unequivocal attitude of the IBA management towards the system solution to information security within its sphere of authority.

Within the concept of this document, the **information security is understood as a stable state of the IBA environment** where controlled levels of **confidentiality, integrity, authenticity and accessibility** of specified (protected) information and other information assets are consistently maintained through a systematic application of the measures taken.

1.2.2. Basic IBA Strategy

The primary mission of Institute biostatistics and analyses Ltd. (hereinafter as „IBA") is „healthy data". The company IBA operates in the healthcare and pharmaceutical industry sectors and perceives the following as its mission or strategy:

- **Providing reliable data management services in the healthcare and life sciences sectors.**
- **Conducting intelligible data analysis for better decision making.**
- **Innovating IT solutions for intuitive and secure use.**
- **Building a strong reputation amongst scientists and medical staff.**

Taking into account the company's core strategy, valid legislative requirements, risk analysis results and quality system review results, the company regularly updates the objectives with aim to ensure the continuous improvement and enhancing the safety of information related to the provided services. These objectives are documented as a separate document „**P04 Plan for improving services**".

1.2.2.1 Objectives of Information Security

In compliance with the normative requirements IBA defines the following security information objectives:

Personnel security:

- include safety factors into the entire lifecycle of employees;
- create and maintain a certain level of security awareness of employees;
- limit attacks, intentional and unintentional human errors;
- limit human errors and their consequences;

Administrative security:

- introduce a single method for safe handling of protected documents throughout their life cycle;

Physical security:

- avoid unauthorized physical access to protected information assets;

Information and communications security:

- avoid unauthorized logical access to protected information assets;

Security of the continuity of activities (business continuity):

- create conditions for renewing the IS operation at shortest possible time, maintaining the integrity and availability of data in the case of failure or breakdown of the IS or other emergencies.

Notes:

The above-mentioned objectives set by the IBA management also include all the partial objectives set out in chapters of Appendix A to ČSN ISO/IEC 27001 standard as results and will result from the interim outcomes and conclusions of assessment processes, risk management and other requirements for information security.

To achieve these objectives, the IBA has taken and further takes the necessary security measures for risk management which are documented in the related standard operating procedures (see chapter Documents and records of this document).

1.2.3. Applicable Principles

Throughout the process of observing the ISMS, the IBA **management declares compliance of the site activities** and behaviour of its employees with the following conclusive principles:

- **direct (clear) responsibility** – specific responsibilities of owners of information assets and other entities providing information security always are and will be defined;
- **necessary knowledge** – all entities participating in providing information security know and will know information security policy, related security documentation and measures laid down therein;
- **integrity** – management of the entire lifecycle of protected data is ensured, i.e. their processing from the time of acquisition or creation to their reliable and traceable disposal;

- **determining levels of information security** – the respective level is always given by the level of the weakest means (link) of information security;
- **adequacy of measures** – security measures taken are always directly proportional to the current value (level) of relevant risks.

1.3. Basic Concepts

IT administrator - the person in charge of the hardware and software tools/devices – he/she deals with their installation, adjustment, etc.

Risk analysis - the process of finding information system assets and their values, threats acting on these assets, vulnerability of the assets, likelihood of the threats and estimation of their consequences.

Security incident – any infringement of the security of the IS or its part, which leads or could lead to damage, both material and abstract.

Information availability – the respective information is accessible to authorized users at the moment when they need it.

Information confidentiality - the respective information is accessible only to those who are authorized to access it.

Information security – preservation of confidentiality, data integrity, data availability and other characteristics such as authenticity, responsibility, undeniability and reliability.

HW = hardware - the technical means for collecting, processing, storing and distributing data including their transmission (e.g. PCs, modems and other active components of computer networks, etc.).

Incident – any event that is not part of the normal functioning of the service and which causes or may cause an interruption of the service supply or degradation of the service quality.

Information - knowledge regarding any objects, e.g. facts, events, things, processes or ideas, including notions that have a specific meaning in the given context.

Information system (IS) - a set of one or more computers, the associated software, peripheral devices, terminals, human operators, physical processes, means for transmitting information, etc. which form an autonomous unit capable of performing information processing or information transfer;

The IS consists of:

- HW - processor, memories, terminals, telecommunications, etc.;
- SW - application programs, operating system, etc.;
- data - data stored in databases, results, output reports, input data, etc.;
- people - staff, users (those qualities and attributes of people that relate to IT security;
- related norms.

Integrity – provision of the accuracy and completeness of information and methods of its processing, i.e. the state where the read information (data) is (are) identical to the original information (data). This means that the information was not unexpectedly changed during its transmission or storage (intentional damage, alteration, errors during transmission).

Policy - a set of rules and procedures for achieving the set goals.

Resources and equipment for information processing – they include all kinds of PCs, organizers, mobile phones, documents and other devices used for work at home or moved outside normal working location:

- PCs, PC peripherals (plotters, printers, etc.);
- mobile computing devices – e.g. laptops, palmtops, laptops, tablets, PDAs, smartphones;
- means for remote working;
- electronic office systems:
- telephones, fax machines, copiers, printers, scanners, multifunction devices, typewriters, dictaphones;
- means for recording and transmission of information:
- cameras, recorders, intercom, memory cards and other devices for transferring information in any other form.

SW (software) - a computer program with the attached documentation and possibly attached data.

User - anyone who directly use ICT facilities and equipment.

Owner (of the assets) - an individual with responsibility for the asset management within its lifecycle. The term "owner" does not indicate the real property of assets in the legal approach.

Record - a document containing the results achieved or providing evidence of activities performed.

Information processing - any operation or set of operations which the IBA and its employees systematically conduct with information, either through automated or other devices; this basically includes information (data) collection, storage on data carriers, disclosure, modification or alteration, retrieval, use, transmission, distribution, publication, hold, exchange, sorting and disposal.

1.4. List of Abbreviations

CEO	Chief Executive Officer
CIO	Chief Information Officer
ČSN	Czech standard
HW	Hardware
IBA	Institute of Biostatistics and Analyses
ICT	Information and Communication Technologies

IEC	International Electrotechnical Committee
IMS	Integrated Management System
IS	Information System
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
ITSM	IT Services Management
P	Plan
PC	Personal Computer
QA	Quality Assurance
QMS	Quality Management System
R	Register
SOP	Standard Operating Procedure
SW	Software

1.5. Related Forms

R20 Risk Assessment Report

P01 Risk Management Plan

P04 Plan for Service Improvement

1.6. List of Appendices

N/A

2. Security Strategy

The IBA management is aware of the fact that no system of information security can be absolutely secure. As an effective way of eliminating relevant risks, it considers the introduction of **efficient risk management system** (see the chapter 4.1 Risk analysis in this document and especially document „**SOP.11 Analysis and Risk Management**").

When managing the risks, the IBA builds and will build on a continuous identification and assessment of risks followed by measures that reduce and eliminate these risks to an acceptable level. An ongoing effort of the IBA management is to solve remaining (residual) risks, especially through measures aimed at early detection of security incidents and actions against these identified incidents.

At the IBA, the **strategy for managing information security**, i.e. existing risks, is therefore based on:

- prevention
- detection
- reaction

Prevention

At the IBA, preventive measures to reduce identified risks are and will be introduced wherever it is possible and economically acceptable.

Preventive measures are always implemented on the basis of risk analysis and are its subsequent step to reduce the risks for individual information assets.

Technical measures are preferable because they work best in the phase of prevention and there is no threat of undesirable side effects.

Organizational measures will be chosen prevention purposes only if an equivalent technical measure does not exist or cannot be used under the given conditions. One of such cases can be particularly a contractual obligation of all partner companies that provide any services for the IBA in the field of information technology.

Detection

At the IBA, the principle of detecting security incidents rests in the adoption and implementation of a system of measures to ensure their signalling, registration and settlement.

For this purpose, all the important activities of users of ICT will be further monitored and recorded in order to allow backward examinations of the development and course of potential security incidents as well as the identification of their possible originators.

The detection is performed mainly using a semi-automatic mechanism at the interface of technical and organizational measures. Most often, it is the result of an analysis of the system for recording incidents and reporting non-standard events to ICT users.

A key factor is timeliness and competency in detecting the security incidents.

Reaction

As a reaction, the IBA means precise operational procedures for investigation, response, resolution and recovery of the system in the event of a detected occurrence of a security incident.

In responding to security incidents, mainly organizational measures will be applied. Technical measures should be of secondary importance.

Emphasis must be again placed on the speed and competency of the immediate response.

Within the settlement of the relevant security incident, the overall response must also include a determination regarding whether and how the risk analysis of the respective assets and possibly other assets will be revised, including follow-up procedures, which will decide on the final countermeasures to be implemented.

3. Powers and Means of Information Security

3.1. Organizational Framework

The following organizational framework has been established in order to effectively manage the ISMS measures under conditions of the IBA:

- IBA CEO;
- Research team for information security (hereinafter referred to as „research team”):
  - Leader of the “research team”- chief information officer (CIO)
  - ICT security manager
  - ICT administrator
  - Quality manager
  - Internal auditor

The „research team” is a conceptual but also executive body of the IBA CEO which, towards the CEO, guarantees the accuracy of measures to address topics of information security, which proposes respective responsibilities and provides that information security is a part of everyday life of the IBA.

For the need of complex solutions to the issues of information security, the CIO in cooperation with the IBA CEO, is entitled to purposefully expand the composition of the team by involving more senior employees or selected specialists of the IBA, or external experts.

3.1.1. Core Competencies of Functions within the ISMS

IBA CEO - management representative for the ISMS:

- is the supreme managing element of the IBA with the highest powers (authorities);
- is a direct supervisor of the "research team" leader and all the executives of the Institute;
- is the owner of the information security policy.

Research team:

- reports to the IBA CEO;
- is a team to perform specific tasks in the field of information security;
- provides methodological assistance to all IBA employees in the field of information security.

Leader of the Research team:

- CIO has the equal powers in point of management information security with the IBA CEO;
- is the main coordinator of all areas of information security at the IBA;
- is responsible for the operation of the "research team".

ICT security manager:

- guarantees security for the team leader in the field of ICT operations.

ICT administrator:

- is a professional and executive guarantor of the team leader in the field of ICT operations.

Quality manager:

- is the executive guarantor of the team leader in the area of management and administration of ISMS documentation.

Internal auditor:

- is an expert and executive guarantor of the IBA CEO in implementing internal audits of the system;
- is a function implementing internal audits and security initiatives in the organization.

Asset owner:

- specifies the category, group, type and scope of the asset;
- proposes the range of authorization regarding the access to the asset;
- proposes a system of measures to protect the asset;

- regarding any changes in the existing assets, he/she closely collaborates with the leader and members of the "research team".

Asset user:

- uses assets only for authorized purposes, in accordance with his/her job duties and this policy;
- observes all issued security measures and guidelines;
- immediately informs his/her direct supervisor, the asset owner and some member of the "research team" about:
  - security incidents, weaknesses and failures of IS/IT;
  - newly detected threats;
  - breaches of security measures;
  - proposals to improve information security.

Risk owner:

- a person or entity with the responsibility and authority to manage the respective risk;
- at the IBA, the initial risk owner is the owner of the given asset to which the risk relates;
- in preparing the risk management plan, the risk can be transferred to another owner.

Note:

Part of the processes and activities in the field of information security is also a continuous assignment of specific competencies to various security roles and functions, and their inclusion in job descriptions of employees.

3.2. Means of Information Protection

In order to fulfil the objectives of the information security policy, the following means (areas) of information protection are defined and will be permanently used:

- personnel security
- administrative security;
- physical security;
- information and communications security;
- security of the continuity of activities (business continuity).

4. Implementation of the Information Security Policy

Within this policy, the IBA management commits to approach the ongoing process of implementation, maintenance and continuous improvement of the ISMS in a creative and systematic manner, and implement information security in areas including:

- participating parties (customers, third parties, outsourcing entities);
- aspects of physical security (object technical and security);
- human resources (human aspects);
- administrative (operating) activity;
- means and equipment for information processing;
- security incidents, events, weaknesses and failures of the ICT;
- ICT communication and operation;
- physical and logical access of persons to the ICT and its subsystems;
- continuity of IBA activities;
- compliance of IBA activities with legal, normative and contractual requirements.

4.1. Risk Analysis

The risk analysis is absolutely crucial and indispensable step towards the establishment of an effective information security system; for this analysis and within the IBA, the following criteria have been set out:

- it must **be in compliance with the normative requirements** in the field of information security;
- it must be **reasonable** and **proportionate** (conform) to the established and current **scope** of the **ISMS**;
- it must continuously **document** the identified and specified **risks** with regard to individual protected information assets or their groups;
- it must ensure that the interpreted **results of risk assessment** are and always will be **comparable and reproducible**;
- it must provide **evidence of continuous improvement** (reduction in risk levels) of the ISMS.

The risk analysis process generally involves activities associated especially with:

- specification and documentation of the protected assets;

- identification of the owners of protected assets;
- determining the extent of their importance, necessity and indispensability for the IBA according to an understandable key;
- assembling the set of potential threats to the protected assets;
- a realistic estimate of the occurrence of these threats;
- implementing the risk calculations;
- interpretation of applicable outputs of the conducted risk analysis.

4.2. Security Measures

In direct relation to and in accordance with the results of the risk analysis, the "research team" further proposes and will propose and implement after approval the measures at 2 basic levels:

1) **Technical measures:**
   - they primarily represent HW or SW technical capabilities which ensure the intended behaviour of the ICT and cannot be simply circumvented;
   - they also include technical and mechanical means to detect, prevent and hinder physical access to protected information assets.
2) **Organizational measures** – they enforce the intended behaviour using means other than technical; they will mainly include:
   - disciplinarily and legally enforceable instruments, usually contractual obligations, amendments to employment contracts, internal directives and other binding regulations for employees;
   - they also include means of personnel security and physical security as well as all control mechanisms and procedures focused on compliance with the above measures.

4.3. Documents and Records

At the IBA, in order to provide evidence of demonstrable compliance with ISMS requirements, all the proposed, adopted and implemented measures are implemented through standard operating procedures, plans, registers and records. At the IBA, this mainly includes the following documents:

- QA.05 Statement of Applicability
- QA.09 Organization Context
- QA.11 ISMS Manual
- SOP.02 Incident and Problem Management
- SOP.07 Monitoring, Measurement, Analysis and Review

- SOP.09 Training in the Field ISMS
- SOP.10 Classification and Management of Assets
- SOP.11 Analysis and Risk Management
- SOP.12 Protection of Personal Data
- SOP.02 Incident and Problem Management
- SOP.16 ICT Operating Procedure
- SOP.17 ICT Security Code
- SOP.23 Internal Audits
- SOP.24 Business Continuity Management
- SOP.25 Management of Resources
- SOP.27 Management of Contracts
- SOP.40 Document Management and Destruction Rules/ Archiving
- R18 Register of Protected Assets
- R20 Risk Assessment Report
- P01 Risk Management Plan
- P06 Emergency Plan for IS Activity Renewal

Complete list of internal control documents is a subject of separate document.

5. Final Provisions

Violation of the principles of the information security policy and related standard operating procedures will be **penalized** in accordance with the established disciplinary code.

The information security policy is subject to regular ISMS reviews (at least once a year).

1. Základní informace

Vedení **Institutu biostatistiky a analýz, s.r.o**. (dále také jen „**IBA**“) chápe řízení bezpečnosti informací jako nedílnou součást celkového řízení společnosti, veškeré své činnosti a zahrnuje zajištění bezpečnosti informací do svého každodenního života.

Systém řízení bezpečnosti informací (dále jen „**ISMS**“) je u IBA vybudován plně v souladu s kriteriálními požadavky aktuální verze normy ČSN ISO/IEC 27001.

Politika bezpečnosti informací je uvozujícím bezpečnostním dokumentem ISMS a je závazná pro všechny zaměstnance IBA a další zainteresované strany vázané k zajištění bezpečnosti příslušnou smlouvou. Každý nový zaměstnanec je s politikou ISMS seznámen ihned po svém nástupu. Za seznámení je zodpovědný manažer kvality.

1.1. Rozsah platnosti

IBA realizuje **ISMS v celém rozsahu** kriteriálních **požadavků** a s naplněním všech principů uvedených v aktuální verzi normy **ČSN ISO/IEC 27001**.

ISMS je zaveden, udržován a trvale zlepšován v celé organizační struktuře IBA na pracovišti Poštovská 68/3, Brno 602 00 a v rozsahu celé činnosti, zahrnující zejména:

- Kompletní řešení projektů klinického výzkumu (registry, NIS, KH);
- Správu dat
- Analýzu dat a správnou interpretaci výsledků;
- Vývoj software nástrojů s ohledem na požadavky zákazníka;
- Vzdělávací aktivity;
- Správu ICT.

ISMS je u IBA vybudován jako přiměřená **součást** již zavedeného **integrovaného systému managementu** (IMS): systému managementu kvality (QMS) a systému managementu a poskytování služeb v oblasti IT (ITSM).

1.2. Účel a cíl

1.2.1. Předmět a účel politiky

Politika bezpečnosti informací IBA představuje souhrn rozhodnutí vedení IBA, jež určují, jak budou stanovené informace a jim příslušná další aktiva chráněna.

Tato politika:

- **vymezuje** základní zásady a principy pro zajištění minimálního bezpečnostního standardu informací (naplnění kriteriálních požadavků aktuální verze normy ČSN ISO/IEC 27001 v podmínkách pracoviště);
- **určuje** hlavní směry a úkoly, kterými budou specifikované požadavky plněny;
- **stanovuje** rámce odpovědností a pravomocí za realizaci cílů bezpečnosti informací;
- **vyjadřuje** zřetelné a jednoznačné stanovisko vedení IBA k systémovému řešení bezpečnosti informací v rámci své působnosti.

Bezpečnost informací je, v pojetí tohoto dokumentu, **chápána jako stabilní stav prostředí** IBA, ve kterém je soustavným uplatňováním souboru opatření trvale zachovávána **řízená úroveň důvěrnosti, integrity, autenticity a dostupnosti** stanovených (chráněných) **informací a dalších informačních aktiv**.

1.2.2. Strategické smýšlení IBA

Základní vizí společnosti Institut biostatistiky a analýz, s.r.o. (dále jen „**IBA**") je poskytovat „**zdravá data"**. Společnost IBA se pohybuje v oblasti zdravotnictví a farmaceutického průmyslu a jako své poslání či strategii vnímá:

- **Poskytovat spolehlivé služby managementu dat v oblasti zdravotnictví a life sciences.**
- **Provádět srozumitelnou analýzu dat umožňující lepší rozhodování.**
- **Inovovat IT řešení pro intuitivní a bezpečné použití.**
- **Budovat silnou reputaci u vědců a zdravotníků.**

S ohledem na základní strategii společnosti, platné legislativní požadavky a výsledky vycházející z analýzy rizik a přezkoumání systému kvality společnost aktualizuje v pravidelných intervalech cíle zajišťující kontinuální rozvoj a navyšování bezpečnosti informací související s poskytovanými službami vedené jako samostatný dokument „**P04 Plán pro zlepšování služeb**".

1.2.2.1 Cíle informační bezpečnosti

V souladu s normativními požadavky vedení IBA definuje následující cíle bezpečnosti informací:

Personální bezpečnost:

- zařazení bezpečnostních faktorů do celého životního cyklu zaměstnance;
- vytvoření a udržování určité úrovně bezpečnostního povědomí zaměstnanců;
- omezení útoků, úmyslných a neúmyslných chyb lidského faktoru;
- omezení chyb způsobených lidským faktorem a jejich důsledků.

Administrativní bezpečnost:

- zavedení jednotného způsobu bezpečného nakládání s chráněnými písemnostmi v celém jejich životním cyklu.

Fyzická bezpečnost:

- zabránění neoprávněným fyzickým přístupům k chráněným informačním aktivům;
- informační a komunikační bezpečnost:
- zabránění neoprávněným logickým přístupům k chráněným informačním aktivům.

Bezpečnost kontinuity činností:

- vytvoření podmínek pro co nejkratší dobu obnovení provozu IS, zachování integrity a dostupnosti dat při výpadku a havárii IS nebo jiné mimořádné události.

Poznámky:

Uvedené cíle stanovené vedením IBA v sobě zároveň zahrnuji i všechny dílčí cíle uvedené v kapitolách Přílohy A normy ČSN ISO/IEC 27001 tak, jak vyplývá a bude vyplývat z průběžných výsledků a závěrů procesů hodnocení a zvládání rizik a dalších požadavků na bezpečnost informací.

K naplnění těchto cílů IBA přijal i nadále přijímá potřebná bezpečnostní opatření pro zvládání rizik, jež jsou dokumentována v navazujících standardních operačních postupech (viz kapitola Dokumenty a záznamy tohoto dokumentu).

1.2.3. Uplatňované principy

Vedení IBA **deklaruje** v celém procesu udržování ISMS **soulad činnosti** pracoviště a chování svých zaměstnanců s následujícími **kriteriálními principy**:

- **adresné odpovědnosti,** kdy jsou a budou vždy stanoveny konkrétní odpovědnosti vlastníků informačních aktiv a ostatních subjektů zajišťujících bezpečnost informací**.**
- **nezbytné znalosti,** kdy všechny subjekty, participující na zajišťování bezpečnosti informací, znají a budou znát politiku bezpečnosti informací, navazující bezpečnostní dokumentaci a opatření v nich stanovena**.**

- **integrity,** kdy je zajištěno řízení celého životního cyklu chráněných informací, tzn. jejich zpracování od okamžiku získání nebo vytvoření až po jejich spolehlivou a doložitelnou likvidaci**.**
- **určující úrovně bezpečnosti informací,** kdy je vždy tato úroveň dána úrovni nejslabšího prostředku (článku) bezpečnosti informací**.**
- **přiměřenosti opatření,** kdy přijímána bezpečnostní opatření jsou vždy přímo úměrná aktuální hodnotě (úrovni) daných rizik**.**

1.3. Základní pojmy

Bezpečnost informací – zachování důvěrnosti, integrity a dostupnosti informací a dalších vlastností jako např. autentičnost, odpovědnost, nepopiratelnost a spolehlivost.

Administrátor IT – osoba pověřená péčí o HW a SW – řeší jejich instalaci, nastavení atd.

Analýza rizik – proces zjišťování aktiv informačního systému a jejich hodnot, hrozeb působící na tato aktiva, zranitelnost aktiv, pravděpodobnost realizace hrozeb a odhad jejich následků.

Bezpečnostní incident – jakékoliv narušení bezpečnosti IS nebo jeho části, které vede nebo by mohlo vést ke škodě jak materiální, tak abstraktní.

Dostupnost informace – zajištění, že informace je pro oprávněné uživatele přístupná v okamžiku její potřeby.

Důvěrnost informace – zajištění toho, že informace je přístupná jen těm, kteří jsou oprávněni k ní mít přístup.

HW – hardware – technické prostředky pro sběr, zpracování, uchovávání a distribuci dat včetně jejich přenosu (např. PC, modemy a další aktivní prvky počítačové sítě apod.).

Incident – jakákoli událost, která není součástí běžného fungování služby, a která způsobí nebo může způsobit přerušení dodávky nebo snížení kvality služby.

Informace – poznatek týkající se jakýchkoliv objektů, např. fakt, událostí, věcí, procesů nebo myšlenek, včetně pojmů, který má v daném kontextu specifický význam.

Informační systém (IS) - množina jednoho nebo více počítačů, s nimi spojeného software, periferních zařízení, terminálů, lidské obsluhy, fyzických procesů, prostředků pro přenos informací atd., které tvoří autonomní celek schopný provádět zpracování informací a/nebo jejich přenos.

IS tvoří:

- HW - procesor, paměti, terminály, telekomunikace atd.;
- SW - aplikační programy, operační systém atd.;
- data - data uložená v databázích, výsledky, výstupní sestavy, vstupní data atd.;

- lidé - personál, uživatelé (ty vlastnosti a atributy osob, které se týkají bezpečnosti IT;
- související normativy.

Integrita – zabezpečení přesnosti a úplnosti informací a metod jejich zpracování. Takový stav, kdy přečtená informace (data) je totožná s původní informací (daty). Tzn., že během přenosu (uložení) informace nedošlo k její neočekávané změně (úmyslným poškozením, pozměněním, chybami při přenosu).

Politika – souhrn pravidel a postupů pro dosahování vytčených cílů.

Prostředky a zařízení pro zpracování informací – zahrnují všechny druhy PC, organizérů, mobilních telefonů, dokumentů a ostatních zařízení, používaných pro práci doma nebo vynášených mimo normální pracovní umístění:

- PC, periferie k PC (plottery, tiskárny apod.);
- mobilní výpočetní prostředky - např. notebooky, palmtopy, laptopy, tablety, PDA, smartphony;
- prostředky pro práci na dálku;
- elektronické kancelářské systémy:
- telefony, faxy, kopírky, tiskárny, scannery, multifunkční zařízení, psací stroje, diktafony;
- prostředky pro záznam a přenos informací:
- fotoaparáty, kamery, záznamníky, intercom, paměťové karty a jiná zařízení umožňující přenášet informace v jakékoliv další podobě.

SW (Software) - programové vybavení - počítačový program s připojenou dokumentací a případně s připojenými daty.

Uživatel – každý, kdo přímo užívá prostředky a zařízení ICT.

Vlastník aktiva – myšlen jedinec, který má vedením IBA přidělenou odpovědnost za řízení aktiva po dobu jeho životnosti. Pojmem „vlastník“ není myšleno skutečné vlastnictví aktiva v právním pojetí.

Záznam – dokument obsahující dosažené výsledky nebo poskytující důkaz o provedených činnostech.

Zpracování informací – jakákoliv operace nebo soustava operací, kterou IBA a jeho zaměstnanci systematicky provádějí s informacemi, a to automatizovaně nebo jinými prostředky; rozumí se tím zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění a likvidace.

1.4. Seznam použitých zkratek

CEO	Jednatel
CIO	Informační ředitel
ČSN	Česká norma

HW	Hardware
IBA	Institut biostatistiky a analýz
ICT	Informační a komunikační technologie
IEC	Mezinárodní elektrotechnická komise
IMS	Integrovaný systém managementu
IS	Informační systém
ISMS	Systém managementu bezpečnosti informací
ISO	Mezinárodní organizace pro standardizaci
IT	Informační technologie
ITSM	Systém managementu poskytovaných služeb IT
P	Plán
PC	Osobní počítač
QA	Jištění kvality
QMS	Systém řízení kvality
R	Registr
SOP	Standardní operační postup
SW	Software

1.5. Související formuláře

R20 Zpráva o hodnocení rizik

P01 Plán zvládání rizik

P04 Plán pro zlepšování služeb

1.6. Seznam příloh

Bez příloh.

2. Bezpečnostní strategie

Vedení IBA si je vědomo skutečnosti, že žádný systém bezpečnosti informací nelze učinit stoprocentně bezpečným. Za účinný způsob eliminace považuje zavedení **efektivního systému řízení rizik** (viz kapitola 4.1 Analýza rizik tohoto dokumentu a zejména pak dokument „**SOP.11 Analýza a řízení rizik**“).

Při řízení rizik IBA vychází a bude vycházet z průběžné identifikace a ohodnocení rizik, na něž navazují opatření, která tato rizika snižují a eliminují na přijatelnou úroveň. Je trvalou snahou vedení IBA řešit ošetřit veškerá rizika zejména opatřeními, která jsou zaměřena na včasnou detekci bezpečnostních incidentů a aktivitami vůči těmto zjištěným incidentům.

Proto je i strategie řízení bezpečnosti informací a vlastně i existujících rizik u IBA založena na:

- prevenci
- detekci
- reakci

Prevence

Všude, kde to je možné a ekonomické, jsou a budou u IBA zavedena preventivní opatření snižující identifikovaná rizika.

Preventivní opatření jsou realizována vždy na základě výsledků analýzy rizik a jsou jejím následným krokem ke snížení rizik pro jednotlivá informační aktiva.

Technická opatření mají přednost, protože ve fázi prevence fungují nejlépe a nehrozí zde nežádoucí vedlejší efekty.

Organizační opatření budou pro prevenci zvolena pouze v případě, že ekvivalentní technické opatření neexistuje nebo je za daných podmínek nelze použít. Jedním z takových případů může být zejména smluvní závazek všech partnerských společností, které poskytují IBA nějakou službu v oblasti informačních technologií.

Detekce

Princip detekce bezpečnostních incidentů spočívá u IBA v přijetí a zavedení soustavy opatření zajišťujících jejich signalizaci, evidenci a vypořádání.

K tomu je a nadále i bude monitorována a zaznamenávána veškerá důležitá činnost uživatelů ICT, aby mohl být zpětně vyšetřen postup a průběh případných bezpečnostních incidentů a odhalen případný původce.

Detekce je prováděna zejména poloautomatickým mechanismem na rozhraní technických a organizačních opatření. Nejčastěji půjde o výsledek analýzy systému pro záznam událostí a hlášení nestandardních událostí uživateli ICT.

Klíčová je včasnost a kvalifikovanost detekce bezpečnostních incidentů.

Reakce

Reakcí IBA rozumí přesný operativní postup pro šetření, reakci, řešení a obnovu systému v případě detekovaného výskytu bezpečnostního incidentu.

Při reakci na bezpečnostní incidenty se budou uplatňovat především organizační opatření. Technická opatření by měla být až druhotná.

Důraz musí být opět položen na rychlost a kvalifikovanost bezprostřední reakce.

Součástí celkové reakce musí být i určení, zda a jakým způsobem bude v rámci vypořádání bezpečnostního incidentu přehodnocena analýza rizik daného aktiva a případně dalších aktiv, včetně návazných postupů, jimiž se rozhodne o konečných protiopatřeních, která budou implementována.

3. Síly a prostředky bezpečnosti informací

3.1. Organizační rámec

Pro efektivní řízení opatření ISMS v podmínkách IBA byl stanoven tento organizační rámec:

- jednatel IBA
- řešitelský tým bezpečnosti informací (dále jen „Řešitelský tým“)
  - vedoucí řešitelského týmu – informační ředitel (CIO)
  - bezpečnostní správce ICT
  - administrátor ICT
  - manažer kvality
  - interní auditor

„**Řešitelský tým**“ je koncepčním, ale i výkonným orgánem jednatele IBA, jež mu garantuje správnost opatření na řešení bezpečnosti informací, navrhuje odpovědnosti a zajišťuje, že bezpečnost informací je součástí každodenního života IBA.

Pro potřeby komplexního řešení otázek bezpečnosti informací je CIO oprávněn v součinnosti s jednatelem účelově rozšiřovat složení týmu o další vedoucí zaměstnance nebo vybrané specialisty IBA, popř. externí odborníky.

3.1.1. Základní kompetence funkcí v ISMS

Jednatel IBA::

- je vrcholným řídícím prvkem IBA s nejvyššími pravomocemi;
- je přímo nadřízen všem vedoucím zaměstnancům společnosti;
- je vlastníkem politiky bezpečnosti informací.

Řešitelský tým:

- je podřízen jednateli IBA;
- je týmem k plnění konkrétních úkolů bezpečnosti informací;
- poskytuje metodickou pomoc všem zaměstnancům IBA v oblasti bezpečnosti informací.

Vedoucí „Řešitelského týmu“:

- je CIO, který má na úrovni rozhodování v oblasti řízení bezpečnosti informací pravomoci srovnatelné s jednatelem společnosti.
- je hlavním koordinátorem zabezpečení informačních systémů u IBA;
- je spoluzodpovědný za činnost „Řešitelského týmu“.

Bezpečnostní správce ICT:

- je garantem bezpečnosti vedoucího týmu v oblasti provozu ICT.

Administrátor ICT:

- je odborným a výkonným garantem vedoucího týmu v oblasti provozu ICT.

Manažer kvality:

- je výkonným garantem vedoucího týmu v oblasti řízení a vedení dokumentace ISMS.

Interní auditor:

- je odborným a výkonným garantem jednatele IBA při provádění interních auditů systému;
- je funkcí realizující interní audity a bezpečnostní iniciativy v organizaci.

Vlastník aktiva:

- specifikuje kategorii, skupinu, druh a rozsah aktiva;
- navrhuje rozsah autorizace přístupu k aktivu;
- navrhuje systém opatření k ochraně aktiva;

- v otázkách jakýchkoliv změn stávajících aktiv úzce spolupracuje s vedoucím a členy „Řešitelského týmu“.

Uživatel aktiva:

- používá aktiva pouze pro schválené účely, v souladu se svými pracovními povinnostmi a touto politikou;
- dodržuje vydané bezpečnostní opatření a pokyny;
- informuje bezprostředně svého přímého nadřízeného, vlastníka aktiva a některého z členů „Řešitelského týmu“ o:
  - bezpečnostních incidentech, slabinách a selháních IS/IT;
  - nově zjištěných hrozbách;
  - porušení bezpečnostních opatření;
  - návrzích na zlepšení bezpečnosti informací.

Vlastník rizika:

- osoba nebo entita s odpovědností a oprávněním řídit riziko
- výchozím vlastníkem rizika na IBA je vlastník daného aktiva, kterého se riziko týká
- v rámci sestavování plánu zvládání rizik může být riziko přeneseno na jiného vlastníka

Poznámka:

Součástí procesů a činností bezpečnosti informací je i průběžné vymezování dalších specifických kompetencí jednotlivým bezpečnostním rolím a funkcím a jejich zakotvení do pracovních náplní zaměstnanců.

3.2. Prostředky ochrany informací

Pro naplnění cílů Politiky bezpečnosti informací jsou stanoveny a budou trvale využívány zejména následující prostředky (oblasti) ochrany informací:

- personální bezpečnost;
- administrativní bezpečnost;
- fyzická bezpečnost;
- informační a komunikační bezpečnost;
- bezpečnost kontinuity činností.

4. Implementace politiky bezpečnosti informací

Vedení IBA se zavazuje přistupovat k probíhajícímu procesu zavádění, udržování a trvalému zlepšování ISMS tvůrčím a systematickým způsobem a realizovat bezpečnost informací v oblastech zahrnujících:

- participující strany (klienti, třetí strany, outsourcující subjekty);
- aspekty fyzické bezpečnosti (objektová a technická bezpečnost);
- lidské zdroje (personální aspekty);
- administrativní (provozní) činnost;
- prostředky a zařízení pro zpracování informací;
- bezpečnostní incidenty, události, slabiny a poruchy ICT;
- komunikace a provoz ICT;
- fyzický a logický přístup osob k ICT a k jejím subsystémům;
- kontinuitu činností IBA;
- soulad činností IBA s právními, normativními a smluvními požadavky.

4.1. Analýza rizik

Analýza rizik je klíčovým a naprosto nezastupitelným krokem pro zavedení efektivního systému informační bezpečnosti a jsou pro ni v rámci IBA stanovena následující kritéria:

- musí být **v souladu s normativními požadavky** v oblasti bezpečnosti informací;
- musí být **vhodná a přiměřená** (vyhovovat) stanovenému aktuálnímu **rozsahu ISMS**;
- musí průběžně **dokumentovat** identifikovaná **a specifikovaná rizika** vůči jednotlivým chráněným informačním aktivum nebo jejich skupinám;
- musí zajistit, že interpretované **výsledky hodnocení rizik** jsou a budou vždy **porovnatelné** a **reprodukovatelné**;
- musí poskytovat **důkazy o trvalém zlepšování** (snižování úrovně rizik) ISMS.

Proces analýzy rizik obecně zahrnuje činnosti spojené zejména:

- se specifikací a zdokumentováním chráněných aktiv;
- s identifikací vlastníků chráněných aktiv;
- se stanovením míry jejich důležitosti, potřebnosti a nepostradatelnosti pro IBA dle srozumitelného klíče;
- se sestavením množiny potenciálních hrozeb vůči chráněným aktivum;
- s reálným odhadem pravděpodobného uplatnění hrozeb;
- s vlastní realizací výpočtu rizik;

- s interpretací využitelných výstupů provedené analýzy rizik.

4.2. Bezpečnostní opatření

V přímé návaznosti a v souladu s výsledky analýzy rizik jsou a nadále i budou „Řešitelským týmem“ navrhována a po schválení implementována opatření ve 2 základních rovinách:

1) **Technická opatření**:
   - představují především technické možnosti HW anebo SW, které zajistí určené chování ICT a nelze je jednoduše nikterak obejít;
   - budou sem spadat i technické a mechanické prostředky k detekci, ztížení a zabránění fyzického přístupu k chráněným informačním aktivum;
2) **Organizační opatření** – vynucující určené chování jinými než technickými prostředky; bude se jednat zejména o:
   - disciplinárně a právně vymahatelné nástroje, nejčastěji smluvní závazky, dodatky k pracovním smlouvám, interní direktiva a další závazné předpisy pro zaměstnance;
   - budou sem spadat i prostředky personální bezpečnosti a fyzická ostraha a všechny kontrolní mechanismy a procedury zaměřené k dodržování výše uvedených opatření.

4.3. Dokumenty a záznamy

Pro potřebu poskytování důkazů o prokazatelném naplňování požadavků ISMS jsou u IBA všechna navržená, přijatá a implementovaná opatření doprovázena cestou standardních operačních postupů, plánů, registrů a záznamů. U IBA se jedná zejména o následující dokumenty:

- QA.05 Prohlášení o aplikovatelnosti
- QA.11 Příručka ISMS
- SOP.02 Řízení incidentů a problémů
- SOP.07 Monitoring, měření, analýzy a přezkoumání
- SOP.09 Výcvik v oblasti ISMS
- SOP.10 Klasifikace a řízení aktiv
- SOP.11 Analýza a řízení rizik
- SOP.12 Ochrana osobních údajů
- SOP.16 Provozní řád ICT
- SOP.17 Bezpečnostní řád ICT
- SOP.23 Interní audity

- SOP.24 Řízení kontinuity činností organizace
- SOP.25 Management zdrojů
- SOP.27 Kontraktační řízení
- SOP.40 Spisový a skartační řád/ Archivace
- R18 Registr chráněných aktiv
- R20 Zpráva o hodnocení rizik
- P01 Plán zvládání rizik
- P06 Havarijní plán pro obnovení činnosti IS

Kompletní seznam interní řízené dokumentace je předmětem samotného dokumentu.

5. Závěrečná ustanovení

Porušování zásad a principů Politiky bezpečnosti informací a navazujících standardních operačních postupů **bude sankcionováno** v souladu se zavedeným disciplinárním řádem.

Politika bezpečnosti informací je předmětem pravidelného (min. 1x ročně) přezkoumání ISMS.