## AZ INFORMÁCIÓBIZTONSÁGI INCIDENSEK KEZELÉSE

### 1 Az információbiztonsági incidensek és javítások kezelése

1.1 Felelősségek és eljárások

A biztonsági események természetét és gyakoriságát a Társaság valamennyi részlegének és az információbiztonsági felelősnek kell folyamatosan figyelemmel kísérnie. Szükség esetén kezdeményezni kell a védelmi intézkedések átalakítását.

1.2 Fogalmak

Az információbiztonsági incidensek olyan egyedi vagy sorozatos információbiztonsági események, amelyek nagy valószínűséggel fenyegetik az információbiztonságot.

Példák:

- a szolgáltatás, a berendezés vagy az eszközök elvesztése;
- vagy túlterhelések (DDos-támadás);
- a fizikai biztonsági rendelkezések megsértése;
- nem ellenőrzött rendszerbeli változások;
- hozzáférési sértések;
- rosszindulatú kód;
- a nem teljes vagy nem pontos működési adatokból eredő hibák;
- a bizalmasság és sértetlenség megsértése;
- az információrendszerekkel való visszaélés

1.3 Információbiztonsági incidensek jelentése

Minden, az IBSZ megismerésére és az abban foglaltak betartására kötelezett felhasználónak kötelessége a késedelem nélkül belül jelezni az informatikai Ügyfélszolgálatnak (security@indivizo.com) minden olyan veszélyforrást, amely az IT biztonságra nézve érdemi fenyegetést jelent vagy jelenthet (a továbbiakban: információbiztonsági incidensek), így különösen a következőket:



## MANAGEMENT OF INFORMATION SECURITY INCIDENTS

### 1 Management of information security incidents and repairs

1.1 Responsibilities and procedures

The nature and frequency of security incidents should be continuously monitored by all of the Company's divisions and the information security officer. If necessary, the restructuring of protective measures should be initiated.

1.2 Definitions

Information security incidents are individual or serial information security incidents that are likely to threaten information security.

Examples:

- loss of service, devices or equipment;
- or overloading (DDos attack);
- violation of physical security provisions;
- unchecked system changes;
- access violations;
- malicious code;
- errors due to incomplete or inaccurate operating data;
- violation of confidentiality and integrity;
- abuse of information systems

1.3 Reporting information security incidents

Any user required to know and comply with the ISR is obligated to notify the IT Customer Service (security@indivizo.com) of any threat source that threatens or could pose a threat to IT security (hereinafter: ‘information security incidents’) without delay, in particular, in the following cases:

- az IBSZ-ben, vagy egyéb belső szabályzatban, jogszabályban előírt IT biztonsági szabályok megszegése, illetve ennek gyanúja;
- a felismert vagy felismerni vélt, az IT biztonságot lényegesen veszélyeztető esemény, különösen:
  - nem nyilvános adat illetéktelen személy általi megismerése,
  - informatikai rendszerekben tárolt adatok illetéktelen személyek általi megváltoztatása, törlése vagy hozzáférhetetlenné tétele,
  - informatikai rendszer működésének, használatának jogosulatlan akadályozása,
  - a Társaság által nem engedélyezett vagy licenccel nem rendelkező szoftver telepítése,
  - fentiek bármelyikére tett kísérlet (pl. felhasználói jelszavak egymás közötti megosztása, vírus-fertőzés),
  - informatikai rendellenes működése;
- a felismert vagy felismerni vélt védelmi gyengeség, biztonsági rés, sérülékenység, hiányos vagy pontatlan szabályozás.

Információbiztonsági incidensnek számít minden, az informatikával kapcsolatba hozható rendellenes működés, fenyegetés, amely az adatok bizalmasságát, sértetlenségét, vagy rendelkezésre állását veszélyezteti.

Az információbiztonsági felelős felelőssége az információbiztonsági incidensről szóló jelzések fogadása, rögzítése, a kockázat értékelése, folyamatban lévő biztonsági incidens vagy annak gyanúja esetén a szükséges kárenyhítő intézkedések megtétele vagy azok kezdeményezése.

Az információbiztonsági incidensekkel kapcsolatos hivatalos információt, tájékoztatást (külvilág vagy a sajtó képviselői felé) csak a Társaság ügyvezető igazgatója által felhatalmazott személy adhat.



- violation or the suspected violation of the IT security rules defined by the ISR or other internal regulations or legislation;
- any event that presumably or actually constitutes a threat to IT security, including especially:
  - disclosure of confidential data to unauthorised persons,
  - modification or erasure of data in information technology systems by unauthorised persons, or making such data inaccessible,
  - unauthorised prevention of the operation or usage of the information system,
  - installation of software that is not authorised by the Company or is unlicensed,
  - an attempt at any of the above (e.g. sharing a user's password with a colleague, or causing a virus infection),
  - IT malfunction;
- recognised or perceived weakness, gap in security, vulnerability, incomplete or inaccurate regulation.

An information security incident is any abnormal operation or threat associated with IT that compromises the confidentiality, integrity, or availability of the data.

It is the responsibility of the information security officer to receive and record notifications of information security incidents, to assess the risk, and take or initiate necessary mitigation measures in the event of an ongoing security incident or the suspicion thereof.

Official information and notification (to the outside world or to the press) related to information security incidents may only be provided by a person authorised by the CEO of the Company.

1.4 Információbiztonsági incidensek felmérése és döntéshozatal

Az információbiztonsági felelős a tudomására jutott információbiztonsági incidensről tájékoztatja az informatikai vezetőt és szükség esetén az ügyvezető igazgatót. Az informatikai vezető a tudomására jutott információbiztonsági incidens kapcsán kezdeményezi a kivizsgálást és erről írásban tájékoztatja az érintett felhasználót és annak közvetlen vezetőjét.

A biztonsági incidenseket soron kívül, késedelem nélkül ki kell vizsgálni, felhasználva a rendelkezésre álló bizonyítékokat. Az informatikai vezető feladata kijelölni a vizsgálatban résztvevő személyeket.

A kivizsgálás kapcsán vizsgálni kell:

- a biztonsági incidens bekövetkezésének okát és körülményeit;
- az esetleges személyi felelősséget;
- az okozott kár mértékét.

Az összegyűjtött bizonyítékokról feljegyzést kell készíteni, amelyben pontosan felsorolásra kerülnek az összegyűjtött bizonyítékok és azok biztonsági incidenssel kapcsolatos tartalmi pontjai. Az elkészült feljegyzéseket fel kell használni a hasonló biztonsági incidensek megelőzésére. A vizsgálat eredményét írásban kell dokumentálni.

1.5 Válasz az információbiztonsági incidensekre

Az információbiztonsági felelős feladata gondoskodni olyan biztonsági nyilvántartás létrehozásáról és vezetéséről, amely tartalmazza a biztonsági incidnesek kapcsán tett bejelentések, a lefolytatott vizsgálatok, valamint a végrehajtott intézkedések adatait.

A nyilvántartásnak minimálisan a következő információkat kell tartalmaznia:

- a biztonsági incidens idejét, helyét és pontos leírását;
- a problémamegoldás során alkalmazott eljárások leírását.

A biztonsági incidensekről szóló feljegyzéseket minden esetben meg kell őrizni.



1.4 Assessment and decision-making on information security incidents

The information security officer is responsible for informing the IT manager and, if necessary, the CEO of the information security incident brought to their attention. The IT manager initiates the investigation in connection with the information security incident they have been made aware of and informs the concerned user and their line manager about it in writing.

Security incidents should be investigated without delay, using the available evidence. It is the responsibility of the IT manager to designate the persons involved in the investigation.

In connection with the investigation, it is necessary to examine:

- the cause and circumstances of the occurrence of the security incident;
- the possible personal responsibility;
- the extent of the damage caused.

A record of the evidence gathered should be prepared, precisely listing the evidence gathered and their content points related to the security incident. The completed records should be used to prevent similar security incidents. The outcome of the investigation shall be documented in writing.

1.5 Response to Information Security Incidents

It is the responsibility of the information security officer to establish and maintain a security record that includes information on the security incident notifications and conducted investigations as well as the actions taken.

The record shall contain at least the following information:

- the time, location and exact description of the security incident;
- a description of the procedures used in problem solving.

Security incident records must always be preserved.

A bizonyítékok sértetlensége, hitelessége kiemelten fontos (pl. peres ügyek bizonyítékaként kívánják felhasználni), minden dokumentumot meg kell őrizni, illetve olyan archiválási- (pl. időbélyegző használata), hozzáférés- ellenőrzési rendszert (ahol minden hozzáférés naplózott) kell bevezetni, melynek kellő bizonyító ereje van.

1.6 Tanulás az információbiztonsági incidensekből

A nyilvántartás adatait fel kell használni:

- a bekövetkezett biztonsági incidens következményeinek enyhítésére;
- a jövőben várható hasonló biztonsági incidensek bekövetkezésének megelőzésére;
- a vizsgálat során feltártakhoz hasonló védelmi gyengeségek kezelésére, a védelmi intézkedések fejlesztésére;
- a kockázatok elfogadható szinten tartására.

1.7 Bizonyítékok gyűjtése

Az információbiztonsági felelős iránymutatásai alapján az adott informatikai rendszerért felelős alkalmazásgazda feladata olyan védelmi intézkedések kialakítása/kialakíttatása, mely lehetőleg automatizált módon (riasztási határértékek meghatározása és beállítása) vagy szabályozott eljárások keretében (pl.: biztonsági napló állományok gyűjtése és kiértékelése) az információbiztonsági incidnes felderítést szolgálja. Ezen intézkedések megvalósítása érdekében a Társaság informatikai rendszereiben a felhasználók tevékenységei közül az alábbiak minimálisan naplózásra kerülnek:

- informatikai rendszerbe történő bejelentkezés (hibás bejelentkezési kísérletek);
- informatikai alkalmazásokhoz és adatokhoz való jogosulatlan hozzáférési kísérletek;
- vírusfertőzések, határvédelmi riasztások;

Az információbiztonsági incidensek felderítéséhez, kivizsgálásához az informatikai vezető és az információbiztonsági felelős kezdeményezésére a fent felsoroltakon kívül indokolt esetben további naplózásokat, rendszermonitorozásokat is végezhetnek időszakosan.



The integrity and authenticity of the evidence is of paramount importance (e.g. to be used as evidence of litigation), all documents must be preserved, and an archiving (e.g. using a time stamp), access control system (where all access is logged) must be introduced with sufficient probative value.

1.6 Learning from IT security incidents

The data of the records must be used:

- for mitigating the consequences of the security incident that has occurred;
- to prevent the occurrence of similar security incidents in the future;
- to address security weaknesses such as those identified during the investigation and to develop security measures;
- to keep the risks at an acceptable level.

1.7 Collection of evidence

Based on the directions provided by the information security officer, the application manager responsible for the given IT system is responsible for the designing/establishment of security measures, which are preferably used within the framework of automated (defining and setting alert limits) or controlled procedures (e.g.: collecting and evaluating security log files) to detect information security incidents. In order to implement these measures, the Company's IT systems minimally log the following activities of users:

- login to the IT system (incorrect login attempts);
- unauthorised access attempts to IT applications and data;
- virus infections, border protection alerts;

In order to detect and investigate information security incidents, in justified cases, they may periodically perform additional logging and system monitoring, upon the initiative of the IT manager and the information security officer.