POVZETEK VARNOSTNIH POLITIK ZA ZUNANJE PARTNERJE/SUMMARY OF ITSEC POLICIES FOR EXTERNAL PARTNERS

Priloga k Standardu / Appendix to standard	
HS - 077 - Krovna varnostna politika	
Verzija / Revision:	**Opis spremembe / Revision description**
1	Prenos na MF.
2	Posodobitev povzetka v skladu s posodobitvijo celotne ITSec dokumentacije.
3	Dodan angleški prevod./English translation added.

Pripravil / Prepared by: Neja Erjavec	**Odobril / Approved by:** Boštjan Tušar
ZAUPNO: Reprodukcija, distribucija in uporaba tega dokumenta, kot tudi posredovanje vsebine drugim brez izrecnega dovoljenja Hidrie, je prepovedana. Avtorske pravice Hidrie. Vse pravice pridržane.	*CONFIDENTIAL: The reproduction, distribution and utilization of this document as well as the communication of its contents to others without expressed authorization is prohibited. Copyright Hidria. All rights reserved.*

POVZETEK VARNOSTNIH POLITIK ZA ZUNANJE PARTNERJE/SUMMARY OF ITSEC POLICIES FOR EXTERNAL PARTNERS

KAZALO:

TABLE OF CONTENTS:

1.00 NAMEN

Seznanitev zunanjih partnerjev o načinih in postopkih varovanja informacij in podatkov v Hidrii.

2.00 VARNOSTNE SMERNICE ZA ZUNANJE PARTNERJE

2.1 Klasificiranje informacij

Nepooblaščeno razkritje zaupnih informacij podjetja lahko resno ogrozi ali najmanj škodljivo vpliva na Hidrio, njene poslovne partnerje ali zaposlene. Gre za znanje, izkušnje in poslovne informacije, ki predstavljajo konkurenčno prednost za družbo ali imajo komercialno vrednost in/ali so povezane s poslovanjem družbe. Zaposlenih, zunanji partnerji in obiskovalci so dolžni varovati zaupne podatke, za katere izvedo med trajanjem razmerja, znotraj ali izven prostorov Hidrie.

Informacije družbe morajo biti zaščitene pred razkritjem tretjim osebam (partnerji, pogodbeni delavci, svetovalci, začasni sodelavci in vsi ostali posamezniki, ki niso zaposleni v družbi) razen, če so tretje osebe posebej pooblaščene preko Pogodbe o ne razkrivanju informacij (NDA) oziroma Izjave o varovanju zaupnosti. Tretjim osebam se lahko informacije podjetja posreduje v primeru, ko obstaja potreba po vedenju in ko je takšna potreba odobrena s strani lastnika informacije.

2.2 Obiskovalci in zunanji izvajalci

Obiskovalce se ob vsakokratnem obisku v Hidrii vpiše v mobilno aplikacijo. Za čas njihovega obiska se jim dodeli identifikacijsko sredstvo (ovratni trak ali priponko z napisom »Obiskovalec«) ter se jih seznani s Smernicami za obiskovalce, ki so dostopne preko QR kode, ki je objavljena na vhodih v podjetje in v mobilni aplikaciji. Vsak obiskovalec elektronsko podpiše Izjavo o varovanju zaupnosti.

Dostop do Hidriinih prostorov je obiskovalcem dovoljen le v spremstvu zaposlenega. V vseh prostorih podjetja je fotografiranje prepovedano. Dovoljeno je izključno ob predhodnem dogovoru z vodjo lokacije. Izjema so pogodbeni partnerji, ki lahko v družbo vstopajo brez spremstva zaposlenih.

1.00 PURPOSE

Informing external partners about the methods and procedures for protecting information and data in Hidria.

2.00 SECURITY GUIDELINES FOR EXTERNAL PARTNERS

2.1 Classification of information

Unauthorized disclosure of the company's confidential information may seriously endanger or at least adversely affect Hidria, its business partners or employees. It is knowledge, experience and business information that represent a competitive advantage for the company or have commercial value and/or are related to the company's operations. Employees, external partners, and visitors are obliged to protect confidential information about which they learn during the duration of the relationship with Hidria.

The company's information must be protected from disclosure to third parties (partners, contract workers, consultants, temporary employees and all other individuals who are not employees of the company) unless the third parties are specifically authorized through a Non-Disclosure Agreement (NDA) or Confidentiality Protection Statement. Company information may be provided to third parties if there is a need for behavior and when such need is approved by the owner of the information.

2.2 Visitors and external partners

Visitors are registered in the mobile application every time they visit Hidria. For the duration of their visit, they are given visitor ID card (neck band or badge with the inscription "Visitor") and they are familiarized with Main Guidelines for visitors in Hidria Company, which are accessible via QR code, which is posted at the entrances to the company and in the mobile application. Each visitor electronically signs the Confidentiality Protection Statement.

Access to Hidria's premises is only permitted for visitors accompanied by an employee. Photography is prohibited on all premises of the company. It is only allowed upon prior agreement with the site manager.
The exception are contractual partners who can enter the company without being accompanied by employees.

Zunanji izvajalci, kot so na primer serviserji in drugi pogodbeni partnerji, ki bodo imeli dostop do občutljivih podatkov, morajo imeti s Hidrio podpisano Pogodbo o nerazkrivanju informacij (NDA) ali Izjavo o varovanju zaupnosti. Za podpis in hranjenje je odgovoren naročnik storitve. Za izvajalce del (serviserje, montažerje ipd.) je potrebno dodatno preveriti, če je z njimi podpisan sporazum o skupnem delovišču. Pisni sporazum ureja postopke za zagotavljanje varnega in zdravega dela v prostorih Hidrie za zunanje izvajalce del.

Pogodbeni partnerji v družbo lahko vstopajo brez spremstva zaposlenih. Ob obisku se jim dodeli priponko zaradi varnosti pri gibanju.

2.3 Upravljanje z uporabniškimi računi

Zunanji partnerji (v kolikor je to potrebno in vnaprej dogovorjeno) za dostop do informacijskih virov Hidrie uporabljajo identifikacijo, ki je sestavljena iz uporabniškega imena in gesla ter dodatnega faktorja avtentikacije (MFA). Uporabniško ime določi administrator. Geslo mora biti kompleksno in se ga spreminja vsake tri mesece.

2.4 Naročanje storitev pri zunanjih izvajalcih

Zunanji izvajalec mora upoštevati pravila upravljanja podatkov Hidrie. Hidria z morebitnim zunanjim izvajalcem najprej sklene Pogodbo o ne razkrivanju informacij (NDA) ali Izjavo o zaupnosti razen, če ni vnaprej določeno, da se uporabijo določila o zaupnosti iz osnovne tipske pogodbe za poslovne partnerje Hidrie. Pri tem se skladno s pogodbo izvaja varovanje informacij skozi celotno obdobje medsebojnega sodelovanja in tudi določeno obdobje po zaključku sodelovanja z zunanjim izvajalcem, kar je lahko od primera do primera različno. V kolikor nabavljena oprema ali storitev informacijskih in telekomunikacijskih tehnologij ni bila predhodno usklajena in odobrena s strani Hidria IT, ta ni dolžna rešitve implementirati v skupno informacijsko komunikacijsko okolje, niti ni dolžna te opreme vzdrževati.
Kadar se pojavi poslovna potreba po dostopu do informacijskih sistemov s strani zunanjih izvajalcev, se najprej, v kolikor se presodi, da je to potrebno izvede analizo in oceno tveganja z ugotovitvami potrebnih varnostnih in nadzornih ukrepov.

External contractors, such as service providers and other contractual partners, who will have access to sensitive data, must have signed a Non-Disclosure Agreement (NDA) or a Confidentiality Protection Statement with Hidria. Hidria is responsible for signing and storing. For work contractors (service technicians, assemblers, etc), it is necessary to additionally check if an agreement on a joint workplace has been signed with them. The written agreement regulates the procedures for ensuring safe and healthy work on Hidria's premises for external contractors.

Contractual partners can enter the company without being accompanied by employees. During the visit, they are given a visitor badge for safety when moving.

2.3 User Account Management

External partners (if necessary and agreed in advance) use identification, which consists of a username and password and an additional authentication factor (MFA), to access Hidria's information resources. The username is determined by the administrator. The password must be complex and changed every three months.

2.4 External partner services

The external contractor must follow Hidria's data protection rules. Hidria first concludes a Non-Disclosure Agreement (NDA) or a Confidentiality Protection Statement with a possible external contractor, unless it is stipulated in advance that the confidentiality provisions from the basic model contract for Hidria's business partners are applied. In accordance with the contract, information protection is carried out throughout the entire period of cooperation and for a certain period after the end of cooperation with the external contractor, which may vary from case to case. If the purchased equipment or service of information and telecommunication technologies has not been previously coordinated and approved by Hidria IT, it is not obliged to implement the solution in a common information and communication environment, nor is it obliged to maintain this equipment.

When there is a business need for access to information systems by external contractors, first, an analysis and risk assessment is carried out with the findings of the necessary security and control measures.

Dostop do informacijskega sistema s strani zunanjih izvajalcev mora biti nadzorovan. Posamični ukrepi nadzora se določijo v soglasju z zunanjim izvajalcem.

Access to the information system by external contractors must be controlled. Individual control measures are determined in agreement with the external contractor.

REFERENČNI DOKUMENTI / REFERENCE DOCUMENTS

HS – 077 – Krovna varnostna politika
HS – 099 – Politika klasificiranja informacij in upravljanja z zaupnimi dokumenti
HS – 100 – Politika upravljanja z uporabniškimi računi in opremo
HS – 107 – Politika E-pošte
HS – 101 – Politika uporabe interneta
HS – 102 – Politika naročanja storitev pri zunanjih izvajalcih
HS – 103 – Politika zaščite pred zlonamerno programsko opremo
HS – 104 – Politika upravljanja neprekinjenega poslovanja
HS – 078 – Politika varovanja v zvezi z osebjem ter dodeljevanja in nadzora dostopov
HS – 105 – Politika prenosne komunikacijske in računalniške opreme ter dela na daljavo
HS – 106 – Politika upravljanja s spremembami v programski opremi
HF – 0303 – Izjava o varovanju zaupnosti
HF – 0051 - Sporazum o zaupnosti - DVOSTRANSKI