Fizična

Vsi zunanji izvajalci in dobavitelji se morajo pred vstopom v območje organizacije seznaniti z varnostnimi pravili in zahtevami.

Varnostna območja:

Javna območja so dostopna vsem, vključno z zunanjimi obiskovalci, brez omejitev.

Interna območja so namenjena samo zaposlenim s potrebami po dostopu, zaščitena s pristopno kontrolo in niso neposredno dostopna od zunaj. Obiskovalci in nepooblaščene osebe lahko dostopajo le ob predhodni najavi in v spremstvu pooblaščenih oseb. Pogodbeni partnerji, kot so vozniki prevozov, poštarji, serviserji opreme, morajo slediti posebnim navodilom glede dovoljenih območij gibanja in varovanja informacij.

Varovana območja so pod strogim nadzorom z dodatnimi varnostnimi ukrepi, kot so posebna pristopna kontrola, protivlomni alarmi in video nadzor. Vstop nepooblaščenim je prepovedan, razen v posebnih primerih s potrditvijo pristojne osebe. Naprave za zajem zvoka in slike so prepovedane, razen s posebnim dovoljenjem direktorja TBP.

Vse tretje osebe, ki vstopajo v interna in varovana območja, morajo nositi oznake za razlikovanje od zaposlenih. Zabeležiti je treba čas vstopa in izstopa ter registrsko številko vozila, če je to potrebno.

Pristopna kontrola ločuje interna in varovana območja od javnih. Pravice dostopa določa kadrovska služba na podlagi minimalno potrebnih pravic. Uporabljajo se brezkontaktne kartice in ključi, z evidenco izdanih ključev in zapisom vstopov in izstopov za varovana območja.

Za **delo v varovanih območjih** veljajo posebne zahteve. Zunanji izvajalci se ne smejo sami nahajati v varovanih območjih. Njihovo delo mora biti ves čas nadzorovano. Prepovedan je vnos lastne IKT opreme. Prepovedan je vnos naprav za zajem slike in zvoka. TBP zagotavlja omarice pred

Physical

All external contractors and suppliers must familiarize themselves with the security rules and requirements before entering the organization's premises.

Safety areas:

Public areas are accessible to everyone, including external visitors, without restrictions.

Internal areas are intended only for employees with access needs, protected by access control and are not directly accessible from the outside. Visitors and unauthorized persons may access only with prior notice and accompanied by authorized persons. Contractual partners, such as transport drivers, postmen, equipment repairers, must follow special instructions regarding permitted areas of movement and information protection.

Protected areas are under strict control with additional security measures such as special access control, burglar alarms and video surveillance. Entry to unauthorized persons is prohibited, except in special cases with the confirmation of a responsible person. Audio and video recording devices are prohibited except with special permission from the General Manager of TBP.

All third parties entering internal and protected areas must wear markings to distinguish them from employees. Entry and exit times and vehicle registration number, if applicable, should be recorded.

Access control separates internal and protected areas from public areas. Access rights are determined by the HR department based on the minimum necessary rights. Contactless cards and keys are used, with a record of issued keys and a record of entries and exits for protected areas.

Special requirements apply to **work in protected areas**. External contractors must not be alone in secured areas. Their work must be supervised at

vhodi v varovana območja, kjer zunanji obiskovalci lahko odložijo opremo, ki je ne smejo vnašati v varovano območje. Vsak obiskovalec mora biti seznanjen s pogoji dela v varovanih območjih in posledicami kršitve politike za delo v teh območjih. **Ne govorimo o poslovnih skrivnostih** z osebami, ki za to niso pooblaščene. **Najdeni dokumenti -** V primeru najdbe nezaščitenih dokumentov, jih takoj predamo varnostni službi TBP.	all times. Bringing your own information communication equipment is prohibited. It is forbidden to bring devices for capturing images and sound. TBP provides lockers in front of entrances to secure areas where outside visitors can leave equipment that they are not allowed to bring into the secure area. Every visitor must be aware of the conditions of work in protected areas and the consequences of violating the policy for working in these areas. **We do not discuss trade secrets** with persons who are not authorized to do so. **Found documents** - If unprotected documents are found, we immediately hand them over to the TBP security service.
Logična **Informacijska varnost v odnosih z dobavitelji** TBP zagotavlja zaščito virov, ki so dostopni dobaviteljem, ter vzdrževanje dogovorjene ravni informacijske varnosti in izvajanja storitev. Pri tem se upošteva in zagotavlja: - ugotavljanje potrebe po dobaviteljih in njihovo izbiro, - vključitev dobaviteljev v sisteme upravljanja (kriteriji), - spremljanje dogovorov o ravni storitve z dobavitelji, - ocenjevanje in preverjanje. **Upravljanje z gesli** - Uporabljamo dovolj dolga gesla, jih NIKOLI ne posojamo ali razkrivamo. Pri izbiri in menjavi uporabniških gesel se upoštevajo naslednja pravila: - izbirati je potrebno gesla z najmanj 8 znakov ustrezne kompleksnosti - znaki gesla naj vsebujejo eno malo in eno veliko črko ter vsaj eno številko - gesla ne vsebujejo šumnikov - gesla je potrebno menjati vsakih 12 mesecev - vsaj 5 zaporednih gesel je neponovljivih	**Logical** **Information security in relations with suppliers** TBP ensures the protection of resources accessible to suppliers, as well as maintenance of the agreed level of information security and service delivery. In doing so, the following is taken into account and ensured: - determining the need for suppliers and their selection, - inclusion of suppliers in management systems (criteria), - monitoring service level agreements with suppliers, - assessment and verification. **Password management** - We use sufficiently long passwords, NEVER lend or disclose them. The following rules are taken into account when choosing and changing user passwords: - it is necessary to choose passwords with at least 8 characters of appropriate complexity, - password characters should contain one lowercase and one uppercase letter and at least one number, - passwords do not contain letters č, š, ž,

- geslo se zaklene za deset minut po petih nepravilnih poizkusih vnosa. Gesla redno menjavamo. **Informacij o podjetju in poslovanju ne delimo z nepooblaščenimi osebami.** **Dostopne pravice** – se redno spremljajo in posodabljajo, vsak uporabnik ima minimalne pravice glede na delovni proces. Dodeljujejo se poimensko za vsakega dobavitelja oziroma vsako tretjo osebo, nikoli za skupino ljudi. **Oddaljen dostop do virov TBP je dovoljen izključno preko poti, ki jih potrdi IT** saj so samo te varne za uporabo in preverjene. Dostopi zunanjih izvajalcev, ki za izvajanje storitev potrebujejo dostop do omrežja TBP, se izvajajo in upravljajo skladno z Navodilom za VPN dostop. (Oddaljeni dostopi so logično in časovno omejeni)	- passwords must be changed every 12 months, - at least 5 consecutive passwords are unrepeatable, - the password is locked for ten minutes after five incorrect input attempts. We change passwords regularly. **We do not share information about the company and operations with unauthorized persons.** **Access rights** - are regularly monitored and updated, each user has minimal rights according to the work process. They are assigned by name for each supplier or each third party, never for a group of people. **Remote access to TBP resources is allowed exclusively through routes approved by IT**, as only these are safe to use and verified. The accesses of external contractors who need access to the TBP network for the provision of services are implemented and managed in accordance with the VPN Access Guide. (Remote accesses are logically and time limited)
Prevare in škodljiva vsebina **Posredovane podatke omejimo na minimalno potrebne** – Ne posredujemo podatkov, za katere menimo, da jih oseba, ki jih zahteva ne potrebuje. **V primeru dvoma o legitimnosti sporočila je potrebno to preveriti pri pošiljatelju ali varnostnem oddelku.**	**Scams and harmful content** **We limit the transmitted data to the minimum necessary** - We do not transmit data that we believe the person making the request does not need. **In case of doubt about the legitimacy of the message, it is necessary to check with the sender or the security department.**
Varovanje prototipov in intelektualne lastnine **Prototipi in ostale poslovne skrivnosti niso naša osebna last –** O njih ne govorimo in ne	**Protection of prototypes and intellectual property**

razkrivamo njihovih lastnosti, pri uporabi pazimo, da so ustrezno zavarovani pred zunanjimi pogledi.	**Prototypes and other trade secrets are not our personal property** - we do not talk about them or reveal their properties, we make sure that they are adequately protected from outside views when using them.

Lenart, 12.01.2024

Predstavnik vodstva za informacijsko varnost/
Information Security Management Representative
Matjaž KOROŠEC

Direktor za kakovost in razvoj/
Quality manager and dev.Dir.
Robert TIRŠ