Obaveze Zastupnika – Tehnički zahtevi

Zastupnik je u obavezi da na sledeći način obezbedi svoj informacioni sistem u cilju sprečavanja zloupotrebe i neovlašćenog pristupa:

- Zastupnik je u obavezi da na odgovoran i siguran način raspolaže osetljivim podacima koje je dobio na korišćenje od strane Platne institucije (korisničke kredencijale, kodove za autorizaciju i verifikaciju i slično).
- Zastupnik je u obavezi da na odgovoran i siguran način čuva i raspolaže osetljivim podacima u koje ima uvid korišćenjem aplikacije Platne institucije.
- Zastupnik je u obavezi da se prizdržava bezbednosnih preporuka platne institucije za korišćenje svog informacionog sistema kao i aplikativnog rešenja platne institucije.
- Zastupnik je u obavezi da obavesti Platnu instituciju o svakom sumnjivom ponašanju aplikacije Platne intitucije na zvaničnu mail adresu Platne institucije.
-

U suprotnom Zastupnik snosi odgovornost ukoliko dodje do neovlašćenog pristupa njegovom informacionom sistemu.

Bezbednosne preporuke za upotrebu svog informacionog sistema i aplikativnog rešenja Platne institucije

Poštovani Zastupnici,

Ovaj dokument sadrži osnovne preporuke za bezbedno korišćenje vašeg informacionog sistema kao i aplikativnog rešenja Platne institucije TNAPP .

Neophodno je da se Zastupnik pridržava ovih uputstava kako bi adekvatno zaštitio uređaje koje koristi za sprovodjenje usluga u ime Platne institucije. Posebnu pažnju treba posvetiti zaštiti i pravilnoj upotrebi podataka i informacija koje su Vam date na korišćenje navedenih usluga.

Prilikom kreiranja korisničkih kredencijala (korisničko ime i lozinka), nemojte koristiti trivijalne kombinacije koje bi mogle biti poznate drugim licima (npr. datumi rođenja članova porodice, brojevi telefona, lični i adresni podaci, imena kućnih ljubimaca i slično).

Zastupnik kao i zaposlena lica kod Zastupnika dužni su da čuvaju tajnost elemenata za potvrdu identiteta, kako oni ne bi došli u posed drugog lica. Čuvanje ovih podataka na mestu dostupnom drugim licima smatra se grubom nepažnjom Korisnika. Ukoliko Zastupnik ili lice koje je zaposleno kod Zastupnika sumnja ili ustanovi da drugo lice ima informaciju o elementima za proveru i potvrdu identiteta, dužno je da odmah po saznanju obavesti Platnu instituciju kako bi se promenili navedeni elementi. Ukoliko dođe do grube nepažnje, Zastupnik snosi štetu nastalu zbog gubitka, neovlašćenog ili neodgovarajućeg korišćenja elemenata za potvrdu identiteta.

Zastupnik ili lice koje je zaposleno kod Zastupnika je dužno da se prilikom upotrebe usluga Platne institucije pridržava Pravila i ovih Bezbednosnih preporuka, kao i pisanih uputstava za Zastupnike i uputstava koja su sastavni deo aplikacija. Korisnik snosi svu štetu nastalu zbog nepridržavanja Pravila i preporuka, koja se mogu preuzeti na internet stranici Platne institucije.

Redovno ažuriranje operativnog sistema računara i aplikacija na Vašem uređaju i pridržavanja bezbednosnih preporuka proizvođača je neophodno za stabilno i bezbedno funkcionisanje računara.

U slučaju da primetite neuobičajeno ponašanje ili izgled aplikacije Platne institcije, kao i neuobičajeno ponašanje računara, molimo Vas da odmah kontaktirate korisnički centar Platne institucije na broj +381 11 4230 201, kao i da pisanim putem obavestite Platnu instituciju o istom na email info@transfernova.com.

Preporučuje se da Zastupnik aktivira bezbednosne funkcionalnosti na računarima na kojima se koristi aplikativno rešenje Platne institucije, kao što su lozinka za pristup nalogu na računaru. Pored korišćenja lozinki za pristup nalozima na računaru, preporučuje se upotreba programa za zaštitu od zlonamernog softvera i virusa (antivirusni programi).

Preporučuje se da Zastupnik ili lice koje je zaposleno kod Zastupnika nikada ne odgovara na poruke ili email-ove u kojima se pošiljalac obraća u ime Transfernova Platne institucije ili u ime Platne institucije traži od Vas da dostavite neki od ličnih podataka. Preporučuje se da kada se neko obraća u ime Platne institucije, Zastupnik ili lice koje je zaposleno kod Zastupnika strogo obrati pažnju sa koje adrese je došao mejl ili poruka. Molimo Vas da takav slučaj odmah prijavite na email adresu info@transfernova.com ili Kontakt centru Transfernova Platne institucije na broj +381 11 4230 201.

Ukoliko dođe do krađe ili gubitka Vašeg mobilnog uređaja, kao i do neovlašćenog pristupa vašem informacionom sistemu potrebno je da odmah obavestite Platnu instituciju na telefon +381 11 4230 201 a potom da se pisanim putem obavesti Platna institucija na mejl info@transfernova.com.

Ukoliko mobilni uređaj podržava upotrebu biometrijskih elemenata (npr. otisak prsta) za otključavanje potrebno je biti obazriv prilikom ustupanja mobilnog uređaja na korišćenje drugim osobama, s obzirom da neovlašćeno mogu sačuvati svoje biometrijske podatke na Vašem uređaju.Preporučuje se da se onemogući snimanje dodatnih biometrijskih elemenata (dodatnog otiska prsta) bez korišćenja PIN-a ili ranije memorisanog biometrijskog podatka.

Preporuka je da se obazrivo obrati pažnja kada pri povezivanju uredjaja na napajanje drugih lica (kao što su tuđi desktop ili notebook računari ili stanice za dopunu mobilnih uređaja na javnim mestima). Povezivanjem mobilnog uređaja na port za napajanje može se pod određenim uslovima i bez Vašeg znanja pristupiti podacima i aplikacijama na uređaju.

Elemente korisničkog naloga kao što su korisničko ime i Lozinka za pristup aplikacijama nemojte saopštavati drugim licima. Nemojte čuvati osetljive podatke (kao što su lozinke, brojevi bankovnih računa, platnih kartica i slično) na Vašim računarima kao ni na mobilnim uredjajima.

Bezbednosne preporuke za upotrebu svog informacionog sistema i aplikativnog rešenja Platne institucije

Zastupnik je dužan da odmah zatraži blokadu naloga u TNAPP aplikaciji u slučajevima gubitka ili postojanja sumnje da su podaci koje je Zastupnik ili lice koje je zaposleno kod Zastupnika dobilo na korišćenje od strane Platne institucije, došli u posed neovlašćenog lica.
Gubitak ili krađu kredencijala, telefona ili drugog mobilnog uređaja koje koristi za pristup aplikacijama koje je Platna institucija dala na korišćenje kao i slučajeve narušavanja bezbednosti, Zastupnik je u obavezi da prijavi Platnoj instituciji na broj +381 4230 201, kao i elektronskom poštom na adresu info@transfernova.com.
Platna institucija će odmah postupiti po prijavi Zastupnika i u zavisnosti od zahteva, Platna institucija može blokirati korisnički nalog u aplikaciji.

Prijava na aplikaciju se od strane Platne institucije po prijemu obaveštenja na neki od prethodno navedenih načina. Korisnik će snositi eventualne posledice zloupotrebe korisničkih kredencijala, odnosno podataka koji definišu korisnički nalog, nastale usled njegove namere ili grube nepažnje.

Blokirani nalog može se deblokirati na zahtev Zastupnika u pisanoj formi. U slučaju neovlašćenog korišćenja korisničkog naloga i neovlašćenog korišćenja korisničkih kredencijala, Zastupnik je dužan da odmah obavesti Platnu instituciju usmeno, a potom i u pisanoj formi na zvaničan mejl Platne institucije, u roku od 24 časa od dana usmenog obaveštenja. Zastupnik ili lice koje je zaposleno kod Zastupnika je dužan da čuva tajnost korisničkog naloga i korisničkih kredencijala, kako ne bi došli u posed neovlašćenih lica. Ukoliko zakonski zastupnik i/ili lice ovlašćeno od strane Korisnika sumnja ili ustanovi da je neko saznao kredencijale, PIN ili lozinku, zakonski zastupnik i/ili ovlašćeno lice od strane je u obavezi da obavesti Platnu instituciju.

U slučaju da Korisnici koji više puta zaredom unesu pogrešne elemente za potvrdu identiteta, sigurnosni mehanizam će, privremeno ili trajno blokirati zaštićene podatke i onemogućiti korišćenje usluge aplikativnog rešenja Platne institucije.

Bezbednost korišćenje računara i konfiguracija

Bezbedan i ispravan uređaj je jedan od preduslova za sigurno obavljanje transakcija i uopšteno korišćenja računara. U nastavku teksta možete pročitati savete za bezbedno konfigurisanje računara :

1.Ažuriranje Sistemskih Softvera i Aplikacija
Redovno ažurirajte operativni sistem na vašim računarima kao i antivirusne programe i sve aplikacije koje koristite. Ova praksa uklanja poznate sigurnosne rupe i poboljšava otpornost sistema.

2.Postavljanje Jakih Lozinki:
Preporuka je da korisnici koriste jake lozinke koje uključuju kombinaciju velikih i malih slova, brojeva i posebnih znakova. Preporučujemo upotrebu dvofaktorske autentikacije (2FA) gde god je to moguće. Takodje, jako je bitno izbegavati čuvati korisničke podatke za pristup aplikaciji u web pretraživaču, kao I na dostupnim mestima poput dokumenata I slično. Takodje za rad na računaru koristiti nalog koji nema administratorske privilegije (korisnički nalog) koji bi trebalo da bude zaštićen Korisničkim imenom i lozinkom.

3.Redovan Backup Podataka:
Redovno pravite sigurnosne kopije važnih podataka i proveravajte njihovu uspešnost vraćanja. Ova praksa pomaže u brzom oporavku u slučaju gubitka podataka usled napada, kvara hardvera ili slučajnih brisanja.

4.Implementacija Firewall-a (zaštitnog zida):
Konfigurišite odnosno podesite firewall kako biste kontrolisali i pratili internet saobraćaj. Ovo pomaže u sprečavanju neautorizovanog pristupa i održava bezbednost mreže.

5.Sigurnosna Politika i Edukacija Zaposlenih:
Razvijte jasnu sigurnosnu politiku koja obuhvata sve aspekte informacione sigurnosti. Održavajte redovne obuke zaposlenima kako bi se podigla svest o sigurnosnim rizicima i pravilnom postupanju. Obratiti pažnju da se Korisnik računara uvek se odloguje sa aplikacija i naloga pre nego napusti računar. Preporuka je da se računar ugasi nakon što se završi sa korišćenjem. Takodje, jako je bitno da se obazrivo i oprezno pristupa nepoznatim internet adresama.

6.Kontrola Prava Pristupa:
Pravilno konfigurišite prava pristupa na sistemu tako da korisnici imaju samo onoliko prava koliko im je potrebno za obavljanje svojih poslova. Ovo smanjuje rizik od neautorizovanog pristupa podacima.

7.Monitorisanje Aktivnosti i Incidenti:
Implementirajte sistem za praćenje i beleženje svih aktivnosti na mreži kako biste brzo identifikovali neobične ili sumnjive aktivnosti. Takođe, razvijte plan za reagovanje na incidente.

8.Enkripcija Podataka:
Koristite enkripciju za zaštitu osetljivih podataka tokom prenosa i skladištenja. Ova mera obezbeđuje dodatni sloj zaštite u slučaju neautorizovanog pristupa.

9.Redovne Provere Sigurnosti:
Periodično sprovodite provere sigurnosti, uključujući penetraciono testiranje i evaluaciju rizika. Ovo vam pomaže da identifikujete potencijalne slabosti i preduzmete odgovarajuće korake za njihovo otklanjanje.

10.Saradnja sa Stručnjacima za Informacionu Sigurnost:
Razmotrite mogućnost angažovanja stručnjaka za informacionu sigurnost kako biste dobili dodatnu podršku i savete prilagođene vašem specifičnom okruženju.