Kent Bank

Politika informacijske sigurnosti

2023.

Namjerno prazna stranica

Sadržaj

1 UVODNE ODREDBE 2

1.1 SVRHA 2
1.2 PODRUČJE PRIMJENE 3
1.3 ZNAČENJE POJMOVA 3
1.4 REFERENTNI DOKUMENTI 6
1.5 ODNOS POLITIKE PREMA DRUGIM OBVEZUJUĆIM AKTIMA I INTERNIM PRAVILIMA BANKE 6

2 SUSTAV UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU 7

2.1 POLITIKA INFORMACIJSKE SIGURNOSTI 7
2.2 UPRAVLJAČKI OKVIR 7
2.2.1 Uprava 7
2.2.2 Voditelj sigurnosti informacijskog sustava 7
2.2.3 Voditelj organizacijske jedinice za informacijsku tehnologiju 8
2.2.4 Službenik za zaštitu osobnih podataka 8
2.2.5 Odbor za upravljanje informacijskim sustavom 8
2.2.6 Vlasnici imovine informacijskog sustava 8
2.2.7 Korisnici informacijskog sustava 8
2.3 INFORMACIJSKA SIGURNOST I LJUDSKI RESURSI 9
2.4 UPRAVLJANJE IMOVINOM INFORMACIJSKOG SUSTAVA 9
2.4.1 Odgovornost za imovinu 9
2.4.2 Klasifikacija informacija 9
2.4.3 Postupanje s medijima za pohranu podataka 10
2.5 UPRAVLJANJE PRISTUPOM 10
2.6 KRIPTOGRAFIJA 11
2.7 FIZIČKA SIGURNOST I SIGURNOST OKRUŽENJA 11
2.8 SIGURNOST OPERACIJA 11
2.9 SIGURNOST KOMUNIKACIJA 11
2.10 NABAVA, RAZVOJ I ODRŽAVANJE SUSTAVA 12
2.11 ODNOSI S DOBAVLJAČIMA 12
2.12 UPRAVLJANJE POVREDAMA INFORMACIJSKE SIGURNOSTI 12
2.13 UPRAVLJANJE KONTINUITETOM POSLOVANJA 12
2.14 USKLAĐENOST 12

3 ZAVRŠNE ODREDBE 13

3.1 TUMAČENJE 13
3.2 NADLEŽNOST I NADLEŽNI SUD 13
3.3 NIŠTETNOST POJEDINIH ODREDBI 13
3.4 PRETHODNO SAVJETOVANJE I STUPANJE NA SNAGU 13

Na temelju *Smjernica EBA-e o upravljanju rizicima IKT-a i sigurnosnim rizicima (EBA/GL/2019/04)* od 28. studenoga 2019., *Odluke o primjerenom upravljanju informacijskim sustavom* (NN 110/2022) od 23. rujna 2022. i *Uredbe (EU) 2022/2554 EUROPSKOG PARLAMENTA I VIJEĆA o digitalnoj operativnoj otpornosti za financijski sektor* od 14. prosinca 2022. Uprava KentBank d.d. (dalje u tekstu „**Banka**"), na sjednici održanoj 24. listopada 2023. godine donosi sljedeću

POLITIKU INFORMACIJSKE SIGURNOSTI

(dalje u tekstu „Politika")

1 UVODNE ODREDBE

Informacije čine ključnu imovinu Banke. Korištenje pravodobnih, točnih i potpunih informacija, s obzirom na njihov utjecaj na poslovanje i upravljačko odlučivanje, ključni su za ostvarivanje poslovnih ciljeva Banke. Svjesna njihova značaja, Uprava Banke kontinuirano upravlja svim rizicima kojima je izložena, a u cilju ispunjenja temeljnih načela informacijske sigurnosti, posebice onim rizicima koji se odnose na informacijsku i komunikacijsku tehnologiju te rizicima koji proizlaze iz njenog korištenja.

1.1 Svrha

Ovom Politikom Uprava Banke uspostavlja sustav te definira osnovna načela upravljanja informacijskom sigurnošću (dalje: **Sustav upravljanja informacijskom sigurnošću**), ponajprije na sljedeće načine:

- usvajanjem ove Politike, Uprava iskazuje svoju krajnju odgovornost za zaštitu informacijske sigurnosti;
- uspostavom adekvatne organizacijske strukture, imenovanjem ključnih funkcija i odbora odgovornih za upravljanje Sustavom informacijske sigurnosti;
- osiguranjem potrebnog broja izvršitelja odgovarajućih vještina te osiguranjem potrebnog proračuna;
- usvajanjem dodatnih internih akata kojima se detaljnije reguliraju pojedina područja Sustava upravljanja informacijskom sigurnošću;
- usvajanjem okvira za upravljanje rizicima informacijske sigurnosti;
- primjenom odgovarajućih upravljačkih, logičkih i fizičkih mjera zaštite informacijskih resursa;
- kontinuiranim podizanjem svijesti Korisnika i osposobljavanjem stručnog kadra u području informacijske sigurnosti;
- aktivnim održavanjem znanja i vještina Uprave Banke koji su im potrebni kako bi mogli razumjeti i procijeniti rizike informacijske sigurnosti, njihov učinak na poslovanje Banke i njima upravljati.

Uspješnom uspostavom Sustava upravljanja informacijskom sigurnošću Banka:

a) postiže visoku razinu sigurnosti kojom je njezina imovina informacijskog sustava na odgovarajući način kontinuirano zaštićena od svih oblika prijetnji;
b) održava strukturirani i sveobuhvatni okvir za identifikaciju i procjenu rizika informacijske sigurnosti, odabir i uspostavu primjerenih mjera za njihovo ovladavanje te unapređuje učinkovitost uspostavljenih mjera;
c) kontinuirano unapređuje svoje upravljačko okruženje i
d) učinkovito postiže i održava zakonsku i regulatornu usklađenost.

Ovom Politikom Uprava Banke izjavljuje i potvrđuje da ciljeve informacijske sigurnosti prihvaća jednako odgovorno kao i ostale poslovne ciljeve te ih promatra u cjelini i usklađuje sa ostalim ciljevima i strategijom Banke.

1.2 Područje primjene

Ova Politika primjenjuje se na cjelokupni informacijski sustav Banke (informacijsku imovinu, informacijsko-komunikacijsku tehnologiju, organizaciju, ljudske resurse, postrojenja i objekte u kojima su smješteni te postupke za prikupljanje, obradu, pohranu, prijenos, zaštitu i zbrinjavanje informacija) uključivo eksternalizirane usluge i sve njegove Korisnike (zaposlenike Banke na neodređeno ili određeno vrijeme, poslovne suradnike i druge osobe koji su na bilo koji način uključene u proslovne procese Banke, članove Nadzornog odbora, dioničare, vanjske dobavljače/pružatelje usluga i njihove zaposlenike te klijente Banke i zaposlenike klijenata pravnih osoba).

Zajedno s *Politikom zaštite osobnih podataka* i *Politikom upravljanja rizikom informacijske sigurnosti* ova Politika definira okvir za uspostavu upravljačkih, logičkih i fizičkih mjera zaštite imovine informacijskog sustava Banke zasnovan na upravljanju rizicima i usklađen sa *Smjernicama EBA-e o upravljanju rizicima IKT-a i sigurnosnim rizicima* te *Uredbi (EU) 2022/2554 Europskog Parlamenta i Vijeća o digitalnoj operativnoj otpornosti za financijski sektor*. Banka primjenjuje i druge smjernice koje proizlaze iz normi informacijske sigurnosti (*ISO 27001:2022*) i dobre prakse upravljanja rizikom informacijske sigurnosti.

1.3 Značenje pojmova

Osim ako je drugačije naznačeno, pojmovi upotrijebljeni i utvrđeni u referentnim dokumentima imaju isto značenje u ovoj Politici.

Pojedini pojmovi u smislu ove Politike imaju sljedeće značenje:

digitalna operativna otpornost znači sposobnost Banke da izgradi, osigura i preispituje svoju operativnu cjelovitost i pouzdanost tako da upotrebom usluga koje pružaju treće strane pružatelji IKT usluga izravno ili neizravno osigura cijeli raspon IKT sposobnosti potrebnih za sigurnost IKT sustava kojima se Banka koristi i kojima se podupire kontinuirano pružanje financijskih usluga i njihova kvaliteta, među ostalim i tijekom poremećaja;

IKT imovina (imovina informacijsko-komunikacijske tehnologije**)** jest softverska ili hardverska imovina za prikupljanje, obradu, pohranu, prijenos, zaštitu i zbrinjavanje informacija koja se nalazi u poslovnom okruženju;

IKT rizik i sigurnosni rizik (rizik informacijske sigurnosti) - rizik koji proizlazi iz korištenja informacijske tehnologije odnosno informacijskog sustava; Rizik gubitaka uslijed povrede povjerljivosti, gubitka integriteta sustava i podataka, neprikladnosti ili nedostupnosti sustava i podataka ili nemogućnosti promjene informacijskih tehnologija (IT-a) unutar razumnog roka i uz razumne troškove u slučaju promjene zahtjeva okruženja ili poslovanja (to jest prilagodljivosti). To obuhvaća sigurnosne rizike koji proizlaze iz neadekvatnih ili neuspješnih internih postupaka ili vanjskih događaja, uključujući kibernetičke napade ili neadekvatnu fizičku sigurnost (EBA/GL/2019/04); Svaka razumno prepoznatljiva okolnost koja se odnosi na upotrebu mrežnih i informacijskih sustava, koja, ako do nje dođe, može dovesti do negativnih učinaka u digitalnom ili fizičkom okruženju te time ugroziti sigurnost mrežnih i informacijskih sustava, svih alata ili procesa koji ovise o tehnologiji, operacija i procesa ili pružanja usluga (DORA);

IKT sustav – vidi „informacijski sustav“;

IKT usluge jesu usluge koje IKT sustavi pružaju Korisnicima; primjeri obuhvaćaju unos podataka, pohranu podataka i obradu podataka te uključuju usluge izvješćivanja, praćenja i podrške za potrebe poslovanja i odlučivanja;

imovina informacijskog sustava – uključuje informacijsku imovinu, postupke za prikupljanje, obradu, pohranu, prijenos, zaštitu i zbrinjavanje informacija (poslovne procese i aktivnosti), IKT imovinu i usluge, organizaciju, ljudske resurse, postrojenja i objekte u kojima su smješteni;

informacijska imovina - jest skup informacija u materijalnom i nematerijalnom obliku koje vrijedi zaštititi (Odluka); *Informacijska imovina uključuje podatke u bazama podataka, datoteke s podacima, programski kôd, sistemsku i aplikacijsku dokumentaciju, korisničke priručnike, planove, interne akte i slično*.

informacijska i komunikacijska tehnologija (**IKT**) jest tehnologija koja omogućuje automatizirano prikupljanje, obradu, generiranje, pohranu, prijenos, prikaz i distribuciju informacija te raspolaganje njima;

informacijska sigurnost - znači očuvanje povjerljivosti, cjelovitosti i dostupnosti informacija. Dodatno, u značenje se mogu obuhvatiti i druga svojstva, poput autentičnosti, neporecivosti, dokazivosti i pouzdanosti;

informacijski sustav (**IKT sustav**) - Informacijski sustav čini sveobuhvatnost tehnološke infrastrukture, organizacije, ljudi i postupaka za prikupljanje, obradu, generiranje, pohranu, prijenos, prikaz te distribuciju informacija kao i raspolaganje njima. Informacijski sustav moguće je definirati i kao međudjelovanje informacijske tehnologije, podataka i postupaka za procesiranje podataka te ljudi koji prikupljaju navedene podatke i njima se koriste;

korisnik informacijskog sustava (**Korisnik**)- sve osobe koje se koriste informacijskim sustavom Banke (zaposlenici, zaposlenici pružatelja usluga, korisnici elektroničkog bankarstva, zaposlenici pravnih osoba koji se koriste informacijskim sustavom Banke itd.);

osobni podaci - svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi (Opća Uredba);

posebne kategorije osobnih podataka - osobni podaci koji otkrivaju rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja ili članstvo u sindikatu, genetski podaci, biometrijski podaci u svrhu jedinstvene identifikacije pojedinca, podaci koji se donose na zdravlje, podaci o spolnom životu ili seksualnoj orijentaciji pojedinca (Opća Uredba);

sustav upravljanja informacijskom sigurnošću (engl. Information Security Management System - **ISMS**) - znači upravljački okvir za sustavni pristup uspostavi, provedbi, radu, praćenju, nadzoru, održavanju i unapređivanju informacijske sigurnosti koji uključuje organizaciju, pravila, odgovornosti, planove, procese i imovinu informacijskog sustava;

temeljna načela informacijske sigurnosti - znači, ovisno o kontekstu, jedno ili kombinaciju načela povjerljivosti, cjelovitosti, raspoloživosti, neporecivosti, dokazivosti, autentičnosti i pouzdanosti;

- **autentičnost** - znači svojstvo koje osigurava da je identitet subjekta zaista onaj za koji se tvrdi da jest;
- **cjelovitost** (integritet) - znači svojstvo informacija (podataka) i procesa da nisu neovlašteno ili nepredviđeno mijenjani;
- **dokazivost** - znači svojstvo koje osigurava da aktivnosti subjekta mogu biti praćene jedinstveno do samog subjekta;

- **neporecivost** - znači svojstvo koje osigurava nemogućnost poricanja izvršene aktivnosti ili primitka informacije (podatka);
- **pouzdanost** - znači svojstvo dosljednoga, očekivanog ponašanja i rezultata;
- **povjerljivost** - znači svojstvo informacija (podataka) da nisu dostupne ili otkrivene neovlaštenim subjektima;
- **raspoloživost** (dostupnost) - znači svojstvo informacija i procesa koje omogućuje pristup tim informacijama i procesima te njihovu upotrebljivost, tj. njihovu dostupnost na zahtjev ovlaštenog subjekta;

vlasnik imovine informacijskog sustava - podrazumijeva univerzalno vlasnika informacijske imovine i/ili vlasnika imovine IKT, ovisno o kontekstu u kojem se koristi;

vlasnik informacijske imovine - znači osoba u okviru čijeg djelovanja je određena informacija nastala. Ovom Politikom pod vlasnikom informacije smatra se vlasnik procesa odnosno odgovorna osoba poslovno-organizacijskog dijela, koji je odgovoran za klasifikaciju informacija, odobravanje i ukidanje pristupa informacijama te određivanje potrebnih mjera zaštite informacija;

vlasnik imovine IKT - osoba odgovorna za nabavu, razvoj, integraciju, izmjene, rad i održavanje IKT imovine informacijskog sustava.

Sljedeća tablica pojašnjava kako dokument treba tumačiti u smislu njegovih verbalnih izraza kao zahtjeva ili preporuka:

Indikacija	Indikator	Značenje
Obveza	(ne) treba, će, mora	označava zahtjeve kojih se treba strogo pridržavati kako bi bili u skladu s dokumentom i od kojih nije dopušteno odstupanje
Preporuka	(ne bi) trebao bi	označava da se među nekoliko mogućnosti jedna preporučuje kao posebno prikladna, bez spominjanja ili isključivanja drugih ili da se određeni tijek radnje preferira, ali nije nužno potreban, ili da se (u niječnom obliku) određena mogućnost ili tijek radnje odbacuje, ali nije zabranjena
Dozvola	(ne) smije	označava način radnje koji je dopušten / zabranjen unutar ograničenja dokumenta
Mogućnost	(ne) može	ukazuje na mogućnost da se nešto (ne) dogodi

1.4 Referentni dokumenti

Sljedeći dokumenti, u cijelosti ili djelomično, normativno su navedeni u ovoj Politici i nužni su za njeno razumijevanje.

Zakonodavni i regulatorni okvir:

- EU GDPR 2016/679 (Uredba (EU) 2016/679 Europskog Parlamenta i Vijeća o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ) (u daljnjem tekstu: **Opća Uredba**)
- Smjernice EBA-e o upravljanju rizicima IKT-a i sigurnosnim rizicima (**EBA/GL/2019/04**)
- **Odluka** o primjerenom upravljanju informacijskim sustavom - HNB (NN 110/2022)
- Uredba (EU) 2022/2554 Europskog Parlamenta i Vijeća o digitalnoj operativnoj otpornosti za financijski sektor i izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014, (EU) br. 909/2014 i (EU) 2016/1011 (u daljnjem tekstu: **DORA**)

Profesionalne norme:

- ISO/IEC 27001:2022(E) Information security, cybersecurity and privacy protection — Information security management systems — Requirements
- ISO/IEC 27002:2022(E) Information security, cybersecurity and privacy protection — Information security controls
- Smjernice za upravljanje informacijskim sustavom u cilju smanjenja operativnog rizika – HNB 2006.

Interni akti:

- Politika zaštite osobnih podataka
- Politika zaštite osobnih podataka zaposlenika
- Politika upravljanja rizikom informacijske sigurnosti

1.5 Odnos Politike prema drugim obvezujućim aktima i internim pravilima Banke

Odredbe Politike namijenjene su osiguravanju visoke i jedinstvene razine upravljanja informacijskom sigurnošću Banke. Banka posvećuje posebnu pažnju zaštiti osobnih podataka kao posebno osjetljivom skupu informacija čija su načela prikupljanja, pohrane, obrade, prijenosa i zbrinjavanja propisane *Općom Uredbom*, *Politikom zaštite osobnih podataka* i *Politikom zaštite osobnih podataka zaposlenika*.

Ova Politika nema utjecaja na postojeće ili buduće obveze ustanovljene zakonima i drugim propisima koje Banka mora poštovati u pogledu informacijske sigurnosti i sigurnosti informacijskog sustava, a koja su šireg opsega od načela utvrđenih ovom Politikom.

Pravila primjenjiva na pojedina područja sustava upravljanja informacijskom sigurnošću detaljnije su uređena pojedinačnim politikama, pravilnicima, procedurama i drugim aktima Banke koji moraju biti usklađeni sa svim relevantnim propisima iz područja informacijske sigurnosti i ovom Politikom.

Banka je usvojila dodatne interne akte za ovo područje i u budućnosti može usvojiti i druge interne akte radi održavanja usklađenosti na pojedinom području poslovanja, pri čemu takvi interni akti nadopunjuju odredbe ove Politike te joj ne smiju proturječiti.

2 SUSTAV UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU

Sustav upravljanja informacijskom sigurnošću skup je pravila, procedura, smjernica te povezanih aktivnosti kojima Banka upravlja u cilju zaštite imovine informacijskog sustava Banke. Banka na taj način ostvaruje sustavni pristup uspostavi, provedbi, radu, praćenju, nadzoru, održavanju i unapređivanju informacijske sigurnosti u svrhu ostvarivanja poslovnih ciljeva i zaštite temeljnih načela informacijskog sustava.

Sustav upravljanja informacijskom sigurnošću temelji se na procjeni i definiranju prihvatljivih razina rizika kako bi se učinkovito postupalo i upravljalo rizicima koji proizlaze iz korištenja informacijskih tehnologija. Primjenom odgovarajućih upravljačkih, logičkih i fizičkih mjera zaštite, Banka umanjuje povezane rizike te kontinuirano nadzire, održava i unapređuje njihovu učinkovitost što doprinosi uspješnosti Sustava upravljanja informacijskom sigurnošću.

2.1 Politika informacijske sigurnosti

Ova Politika temeljni je okvir za upravljanje informacijskom sigurnošću i odražava općeprihvaćena (high-level) načela sigurnosti.

Uprava Banke može donositi i druge interne akte radi zaštite informacijske imovine, sustava i ljudi u skladu s poslovnim potrebama i sigurnosnim zahtjevima.

2.2 Upravljački okvir

Uprava Banke uspostavlja ovom Politikom organizacijski i upravljački okvir i definira odgovornosti ključnih funkcija u Sustavu upravljanja informacijskom sigurnošću.

Ključne funkcije u upravljanju informacijskom sigurnošću čine Uprava, Voditelj sigurnosti informacijskog sustava, Voditelj organizacijske jedinice za informacijsku tehnologiju (Direktor Sektora informatike), Službenik za zaštitu osobnih podataka, Odbor za upravljanje informacijskim sustavom, Vlasnici imovine informacijskog sustava i Korisnici.

Odgovornosti ključnih funkcija i ostalih uloga u sustavu upravljanja informacijskom sigurnošću definirane su u nastavku. Sveukupne odgovornosti pojedinih uloga propisane su internim aktima koji detaljno uređuju pojedina područja upravljanja informacijskom sigurnošću Banke.

2.2.1 Uprava

Uprava Banke uspostavlja adekvatnu organizacijsku strukturu i ključne funkcije, imenuje Odbor za upravljanje informacijskim sustavom i definira njihov djelokrug rada, ovlasti i odgovornosti, donosi strategiju informacijskog sustava Banke, strateške i operativne planove te nadzire njihovo provođenje.

2.2.2 Voditelj sigurnosti informacijskog sustava

Voditelj sigurnosti informacijskog sustava nadzire i koordinira aktivnosti vezane uz informacijsku sigurnost, primjenjuje dobre prakse i prihvaćene standarde informacijske sigurnosti te savjetuje korisnike u svezi informacijske sigurnosti.

Voditelj sigurnosti informacijskog sustava neovisna je kontrolna funkcija odvojena od operativnih postupaka vezanih uz informacijske i komunikacijske tehnologije. Izravno je odgovoran Upravi Banke.

2.2.3 Voditelj organizacijske jedinice za informacijsku tehnologiju

Voditelj organizacijske jedinice za informacijsku tehnologiju upravlja, nadzire i koordinira njenim radom, primjenjuje dobre prakse i prihvaćene standarde u uspostavi i provođenju procesa upravljanja informacijskim sustavom s ciljem osiguranja primjerene funkcionalnosti i djelotvornosti informacijskog sustava.

2.2.4 Službenik za zaštitu osobnih podataka

Službenik za zaštitu osobnih podataka odgovoran je za provođenje svih mjera i aktivnosti usmjerenih na ostvarivanje ciljeva *Politike zaštite osobnih podataka*, provedbu zakonskih, podzakonskih i drugih obvezujućih akata na području zaštite osobnih podataka. Samostalan je i neovisan u svom radu i ovlašten je poduzimati sve potrebne aktivnosti i mjere kako bi se osigurala usklađenost poslovanja Banke s propisima o zaštiti osobnih podataka. Izravno je odgovoran Upravi Banke.

2.2.5 Odbor za upravljanje informacijskim sustavom

Odbor za upravljanje informacijskim sustavom savjetodavno je tijelo Upravi Banke čija je uloga praćenje i nadziranje upravljanja informacijskim sustavom i povezanim aktivnostima u smislu usklađenosti s regulativom, poslovnim ciljevima i strateškim planom Banke. Uz navedeno, uloga Odbora je i koordinacija inicijativa vezanih uz razvoj informacijskog sustava, optimizacija troškova i upravljanje

2.2.6 Vlasnici imovine informacijskog sustava

U smislu odredbi ove Politike, Vlasnik imovine informacijskog sustava je odgovorna osoba poslovno-organizacijske jedinice u čijoj nadležnosti se nalazi predmetna imovina.

2.2.7 Korisnici informacijskog sustava

Korisnici informacijskog sustava Banke odgovorni su za poštivanje odredbi ove Politike i drugih akata Banke (interni akti, opći uvjeti, upute).

2.3 Informacijska sigurnost i ljudski resursi

Zaposlenici i ostali Korisnici informacijskog sustava Banke trebaju ispunjavati sigurnosne kriterije, raspolagati potrebnim vještinama za uloge koje obnašaju i razumjeti svoje odgovornosti.

U obnašanju svojih aktivnosti trebaju biti svjesni rizika povezanih s informacijskom sigurnošću i primjenjivati propisane mjere zaštite.

Uprava Banke uspostavila je program obrazovanja u cilju informiranja, osvješćivanja i educiranja Korisnika informacijskog sustava o promjenama funkcionalnosti i sigurnosnih obilježja informacijskog sustava Banke te prijetnjama informacijskoj sigurnosti i primjerenim načinima zaštite.

Program obrazovanja:

- Obuhvaća sve Korisnike informacijskog sustava Banke;
- Razvija i održava znanja i vještine Korisnika na primjerenoj razini kako bi mogli obavljati radne zadaće na djelotvoran i siguran način;
- Upoznaje Korisnike s internim politikama, procedurama i ostalim postupcima kojih se moraju pridržavati kako bi se točno utvrdili zadaci, opseg djelovanja i osobna odgovornost svakog Korisnika;
- Uspostavlja i unapređuje svijest o potrebi zaštite imovine informacijskog sustava Banke;
- Razvija i održava znanja potrebna da bi se funkcionalnost i sigurnost informacijskog sustava zadržale na zadovoljavajućoj razini tijekom njegova životnog vijeka.

Nepridržavanje propisanih mjera zaštite i povrede informacijske sigurnosti podložne su sankcijama u skladu s relevantnim zakonskim, statutarnim, regulatornim ili ugovornim odredbama.

2.4 Upravljanje imovinom informacijskog sustava

2.4.1 Odgovornost za imovinu

Banka aktivno upravlja imovinom informacijskog sustava i provodi mapiranje svojih poslovnih funkcija, IKT sustava i IKT imovine koja podržava te funkcije kako bi utvrdila njihovo pojedinačno značenje i međuovisnost s IKT rizicima te kako bi mogla primjereno upravljati imovinom informacijskog sustava koja podržava kritične poslovne funkcije i procese.

Banka imenuje vlasnike imovine informacijskog sustava koji su odgovorni za njenu zaštitu tijekom cjelokupnog životnog vijeka.

2.4.2 Klasifikacija informacija

Banka klasificira informacijsku imovinu u skladu sa zakonskim i regulatornim zahtjevima, njenom vrijednošću te rizikom i stupnjem osjetljivosti na moguće posljedice narušavanja povjerljivosti, autentičnosti, cjelovitosti i raspoloživosti.

Stupanj osjetljivosti procjenjuje se konzistentno, na razini cijele organizacije, u skladu sa definiranim kriterijima za procjenu utjecaja i klasifikaciju informacija.

Banka označava informacijsku imovinu po kriteriju povjerljivosti. Označavanje se provodi za informacije u fizičkom i elektroničkom obliku. Iznimke su one informacije koji se uručuju klijentima po bilo kojoj osnovi i informacije objavljene na javnim internetskim stranicama Banke.

Svi Korisnici informacijskog sustava Banke trebaju koristiti sljedeće oznake prilikom klasifikacije ili postupanja s informacijama Banke i štititi njihovu povjerljivost u skladu s propisanim načelima:

Oznaka	Načelo	Primjer
Javne informacije	Informacije bez ograničenja pristupa.	Javno dostupni registri, publikacije, informacije objavljene na internetskim stranicama Banke (npr. javno dostupne politike, opći uvjeti, brošure s ponudom proizvoda Banke, financijska i bonitetna izvješća i sl.) ili druge publikacije namijenjene klijentima i široj javnosti.
Interne informacije	Informacije dostupne svim zaposlenicima banke i ostalim korisnicima s odobrenjem.	Informacije za podršku redovnom poslovanju namijenjene zaposlenicima Banke i ostalim korisnicima s odobrenjem – dobavljačima, pružateljima usluga i drugim osobama koji su na bilo koji način uključene u proslovne procese Banke, sukladno poslovnim potrebama.
Povjerljive informacije	Informacije dostupne ovlaštenim grupama korisnika (najčešće timovi ili organizacijske jedinice, uključujući ovlaštene vanjske strane).	Informacije iz poslovanja zaštićene na temelju vlasničkih, etičkih ili pravnih ograničenja (poslovna ili bankarska tajna – informacije o klijentima, zaposlenicima, računima, stanjima i prometima računa, povezanim osobama i sl.), osobni podaci.
Tajne informacije	Najosjetljivije informacije iz poslovanja koje su zakonom, regulatornim propisom, odlukom Banke ili vlasnika informacije određene tajnima, pristup kojima se odobrava na individualnoj osnovi.	Posebne kategorije osobnih podataka, podaci o plaćama, lozinkama i PIN-ovima, posebno osjetljive poslovne informacije i sl.

Ukoliko Korisnik sazna ili dođe u posjed informacije koja mu nije namijenjena, događaj treba prijaviti kao povredu informacijske sigurnosti u skladu s odredbama Članka 2.12 ove Politike, a zaprimljenu informaciju predati Vlasniku.

2.4.3 Postupanje s medijima za pohranu podataka

Svi Korisnici informacijskog sustava Banke trebaju koristiti medije za pohranu podataka na način kojim će spriječiti neovlašteno otkrivanje, izmjenu, brisanje ili uništavanje podataka pohranjenih na medijima.

Informacije pohranjene na medijima za pohranu podataka treba štiti u skladu s njihovom klasifikacijskom oznakom.

Medije za pohranu treba u potpunosti očistiti od podataka prije ponovne upotrebe ili uništiti u postupku zbrinjavanja.

2.5 Upravljanje pristupom

Banka je propisala i primjenjuje odgovarajuće mjere zaštite kako bi spriječila neovlašteni pristup resursima informacijskog sustava, utvrdila autentičnost Korisnika i osigurala dokazivost i neporecivost njihovih aktivnosti.

Svakom korisniku informacijskog sustava Banka dodjeljuje jedinstven korisnički identitet i provjerava njihovu autentičnost na način koji, ovisno o osjetljivosti informacija kojima se pristupa, može uključivati više faktora autentifikacije.

Pristup resursima informacijskog sustava dodjeljuje se u skladu s poslovnim zahtjevima, samo do razine koja omogućava izvršavanje radnih zadataka Korisnika, skladno njihovoj ulozi i stupnju osjetljivosti informacija kojima pristupaju. Promjenom ili prestankom svrhe zbog koje su dodijeljena, prava pristupa se ažuriraju ili ukidaju.

Korisnicima s pravom povlaštenog pristupa resursima informacijskog sustava Banke uvedene su dodatne kontrole koje umanjuju rizik od namjerne ili nenamjerne zlouporabe sustava. Razgraničenje dužnosti korisnika s pravom povlaštenog pristupa provodi se tamo gdje je to moguće.

Udaljeni pristup informacijskom sustavu, uključivo udaljeni rad, ograničen je na ovlaštene korisnike uz nužnu primjenu dodatnih mjera zaštite.

2.6 Kriptografija

Banka je propisala i primjenjuje kriptografske metode i alate za učinkovitu kriptografsku zaštitu informacijske imovine koju štiti u skladu s njenom vrijednošću te rizikom i stupnjem osjetljivosti na moguće posljedice narušavanja povjerljivosti, cjelovitosti i raspoloživosti.

Svi korisnici informacijskog sustava Banke trebaju štititi klasificirane informacije u pohrani, obradi i prijenosu u skladu s propisanim razinama zaštite.

2.7 Fizička sigurnost i sigurnost okruženja

Banka provodi mjere fizičke zaštite imovine informacijskog sustava od neovlaštenog pristupa i opasnosti povezanih s okolišem.

Uređaji za obradu podataka smješteni su u sigurnim područjima, zaštićeni od okolišnih i fizičkih prijetnji, neovlaštenog pristupa, oštećenja i ometanja.

Uspostavljene su slojevite unutarnje i vanjske sigurnosne kontrole kako bi se odvratio ili spriječio neovlašteni pristup i zaštitila imovina, posebno ona koja je kritična ili osjetljiva.

2.8 Sigurnost operacija

Banka osigurava ispravno i sigurno funkcioniranje informacijskog sustava:

- Dokumentiranjem operativnih postupaka,
- Upravljanjem promjenama i kapacitetima,
- Razdvajanjem razvojnih, testnih i produkcijskih okolina,
- Primjenom sustava za zaštitu od zlonamjernog softvera,
- Izradom sigurnosnih kopija podataka i testiranjem oporavka,
- Bilježenjem i praćenjem operativnih i sistemskih zapisa komponenti informacijskog sustava,
- Identificiranjem i tretiranjem ranjivosti sustava

2.9 Sigurnost komunikacija

Banka je propisala i provodi mjere zaštite komunikacija kako bi zaštitila podatke unutar svoje računalne mreže te osigurava alate i smjernice za siguran prijenos podataka internom mrežom i s vanjskim entitetima, u skladu s klasifikacijom i zahtjevima rukovanja povezanim s tim informacijama.

2.10 Nabava, razvoj i održavanje sustava

Zahtjevi za sigurnost informacijske imovine, usluga i sustava IKT-a procjenjuju se i definiraju tijekom pripreme poslovnih zahtjeva za novim ili izmjenama postojećih funkcionalnosti informacijskog sustava. Mjere za ublažavanje identificiranih rizika provode se gdje je to potrebno.

Sve promjene u sustavu provode se planirano i kontrolirano. Operativne (produkcijske) IKT usluge i sustavi odvojeni su od razvojnih i testnih okruženja kako bi se umanjio rizik od sigurnosnih propusta ili nedostupnosti IKT usluga i sustava.

Korištenje resursa prati se, prilagođava i izrađuju projekcije budućih zahtjeva za kapacitetom kako bi se osigurale potrebne performanse sustava.

2.11 Odnosi s dobavljačima

Pri uspostavljanju odnosa s dobavljačima razmatraju se zahtjevi informacijske sigurnosti kako bi se osigurala zaštita imovine dostupne dobavljačima.

Aktivnost dobavljača prati se, a njihova prava revidiraju u skladu s vrijednošću imovine i povezanim rizicima.

2.12 Upravljanje povredama informacijske sigurnosti

Banka je uspostavila okvir za upravljanje povredama informacijske sigurnosti s ciljem pravovremenog i učinkovitog odgovora na neplanirane događaje koji mogu ugroziti temeljna načela informacijske sigurnosti.

Korisnici informacijskog sustava Banke dužni su prijaviti svaki događaj ili pojavu za koje sumnjaju da predstavlja povredu informacijske sigurnosti ili ranjivost sustava.

Vanjski Korisnici (vanjski suradnici, dobavljači, klijenti i dr.), događaj trebaju prijaviti Voditelju sigurnosti informacijskog sustava na adresu elektroničke pošte vsis@kentbank.hr.

Svi prijavljeni događaji procjenjuju se i u ovisnosti o njihovu karakteru klasificiraju kao incidenti informacijske sigurnosti.

2.13 Upravljanje kontinuitetom poslovanja

Banka je uspostavila okvir za upravljanje kontinuitetom poslovanja kao jednim od ključnih elemenata upravljanja sigurnošću poslovanja i smanjenja operativnih rizika, definirala uloge, odgovornosti i ciljeve upravljanja kontinuitetom poslovanja.

U okviru procesa upravljanja kontinuitetom poslovanja, Banka priprema, redovito usklađuje i testira planove kontinuiteta poslovanja i oporavka informacijskog sustava Banke.

Primjenom odgovarajućih zaštitnih mjera, Banka osigurava otpornost na gubitak dostupnosti i cjelovitosti informacijske imovine i sustava.

2.14 Usklađenost

Banka poštuje i uskladila je svoje djelovanje s važećim zakonima RH i EU, kao i svim drugim regulatornim zahtjevima i ugovornim obvezama.

Neiscrpan sažetak zakona, regulatornih i ugovornih obveza koje doprinose obliku i sadržaju ove Politike navedeni su u poglavlju 1.4 Referentni dokumenti.

Povezane politike i drugi interni akti detaljno opisuju ostale primjenjive zakonodavne uvjete i pružaju daljnje detalje o obvezama koje proizlaze iz pozitivnih zakonskih propisa i regulatornih zahtjeva.

3 ZAVRŠNE ODREDBE

Svi Korisnici informacijskog sustava Banke trebaju biti upoznati s odredbama ove Politike i pridržavati ih se.

Nepridržavanje odredbi ove *Politike* i drugih akata Banke od strane Korisnika može predstavljati temelj za raskid poslovnog odnosa, materijalnu i kaznenu odgovornost.

3.1 Tumačenje

Ova Politika tumači se sukladno zakonodavnom i regulatornom okviru definiranom u točki 1.4 Referentni dokumenti i primjenjivom zakonodavstvu Republike Hrvatske i Europske Unije.

3.2 Nadležnost i nadležni sud

Za sve eventualne sporove proizašle iz povrede informacijske sigurnosti primjenjuju se zakoni i drugi propisi primjenjivi u Republici Hrvatskoj.

Sud nadležan za rješavanje u sporu je stvarno nadležni sud prema sjedištu Banke.

3.3 Ništetnost pojedinih odredbi

U slučaju da se utvrdi da je određena odredba ove Politike ništetna, takva odredba će se zamijeniti odredbom koja u najvećoj mogućoj mjeri odgovara namjeri koju je Banka htjela postići ništetnom odredbom te isto ne povlači ništetnost cijele Politike.

3.4 Prethodno savjetovanje i stupanje na snagu

Ova Politika stupa na snagu 24. listopada 2023., danom njenog usvajanja od strane Uprave Banke.

Ovu Politiku Banka će revidirati prema potrebi.