Na osnovu ovlašćenja proisteklih iz člana 40. Osnivačkog akta BDD Convest a.d. Novi Sad, te na osnovu odluke o sprovođenju mera i aktivnosti u cilju zaštite i kontrole informacionog sistema BDD Convest a.d. Novi Sad i u skladu sa tačkom 139. Pravila poslovanja Centralnog registra, direktor BDD Convest a.d. Novi Sad dana 12.08.2014. godine donosi sledeću:

PROCEDURU

za pristup informacionom sistemu Centralnog registra, analizu aktivnosti i postupak kontrole korisničkih prava pristupa i postupanja zaposlenih u cilju sprečavanja neovlašćenog korišćenja smart kartica Centralnog registra

Lista izmena

Verzija/broj izmena	**1/0**	**1/1**	**1/2**	**1/3**	**1/4**	**1/5**
Datum primene	2014-08-12					
Sve izmenjene strane od ukupnog broja strana						
Autor:	Danijela Budimir					
Overio:	Đorđe Čanak					
Predlagač:	-					

Izvršni direktor
Danijela Budimir

Generalni direktor
Đorđe Čanak

Generalni direktor

Đorđe Čanak

.

1. UVOD - Podela informacionog sistema BDD Convest a.d. Novi Sad

Registracija aktivnosti u informacionom sistemu vrši se na više različitih načina. Svaki od ovih načina se odnosi na tačno određene aktivnosti i na tačno određeni deo informacionog sistema. U tom smislu možemo izvršiti podelu informacionog sistema u odnosu na vrstu, način i mesto registracije aktivnosti u njemu, i to na sledeće delove:

- Radne stanice i serveri
- Deljeni mrežni resursi (deljeni mrežni prostor za smeštaj podataka, mrežni štampač, internet servis i servis elektronske pošte)
- Program: „Back Office 2004“ za kompletno praćenje brokerskog i dilerskog poslovanja BDD Convest
- Program: „Klijent centar“ za trgovanje na Beogradskoj Berzi
- Program: „BSE Prospekt“ Beogradske berze za administraciju prospekata emitenata HoV
- Program: „Web aplikacija CRHoV“ i »Beoklijent« za vođenje računa HoV klijenata
- Program: „Aukcijska platforma“ Web servis Trezora NBS za trgovanje trezorskim zapisima
- Program: „IRIS“ za knjigovodstvo i računovodstvo
- Program: „Ibank FX client“ program za online platni promet preko interneta

U svakom od navedenih delova informacionog sistema vrši se registracija, analiza i kontrola aktivnosti koje korisnici obavljaju u tom delu informacionog sistema, tako da je neophodno definisati procedure za registraciju, analizu i kontrolu ovih aktivnosti unutar svakog dela posebno.

2. Registrovanje aktivnosti u delu informacionog sistema – program „Web aplikacija CRHoV“ i „beoklijent“ Centralnog registra (u daljem tekstu informacioni sistem centralnog registra)

Informacioni sistem Centralnog registra je instalisan samo na onim radnim stanicama koje koriste korisnici koji imaju ovlašćenje za pristup ovom sistemu. U samom sistemu definistani su korisnički nalozi sa svojim korisničkim imenom i lozinkom. Prilikom svakog pristupa sistemu, korisnik mora uneti svoje korisničko ime i lozinku, i ubaciti svoju elektronsku karticu (smart card) u čitač ili ne može koristiti sistem. Na osnovu unetog korisničkog imena i lozinke, kao i podataka koji se nalaze na korisničkoj elektronskoj kartici, definisane su aktivnosti koje korisnik može vršiti u sistemu, u skladu sa njihovim ovlašćenjem za pristup informacionom sistemu. Registrovanje određenih aktivnosti u sistemuu se vrši automatski, beleženjem vremena i korisničkog naloga koji izvršava ove aktivnosti.
Dakle, procedura registrovanja aktivnosti u Informacionom sistemu Centralnog registra se svodi na unos korisničkog imena i lozinke i ubacivanje elektronske kartice sa njihovim pristupnim podacima na početku korišćenja programa, kao i odjavljivanje iz programa i uklanjanje njihove elektronske kartice iz čitača i njeno odlaganje na bezbednu lokaciju na kraju korišćenja programa. Određene aktivnosti koje korisnik vrši u programu se beleže u logovima programa. Korisnici moraju biti pažljivi i voditi računa da ne dođe do otkrivanja kombinacije njihovog korisničkog imena i lozinke, i otuđenja njihove elektronske kartice kao i da svaki put kada napuste radno mesto izvrše odjavljivanje iz programa, i odlaganje elektronske kartice na bezbedno mesto, kako neko drugo lice ne bi izvršilo aktivnosti u programu sa njihovim nalogom u njihovom odsustvu.

U skladu sa Ovlašćenjem „Convest-ZIS-D-12-001“ i Odlukom generalnog direktora daje se ovlašćenje za pristup i rad na programima Informacionog sistema Centralnog registra. Predmetna Odluka mora biti objavljena na vidnom mestu u poslovnim prostorijama BDD Convest (u daljem tekstu korisnik informacionog sistema centralnog registra)

U slučaju prestanka zaposlenja ovih lica ili njihovog prelaska na drugo radno mesto koje ne zahteva pristup programima Informacionog sistema Centralnog registra, korisnik informacionog sistema je u obavezi da smart kartice vrati Centralnom registru i zatraži poništenje certifikata na smart kartici. Isto tako dužan je i da o svakoj promeni lica koja su ovlašćena za pristup i obavljanje poslova u informacionom sistemu centralnog registra bez odlaganja u pisanoj formi obavesti Centralni registar i da navedeni akt objavi na vidnom mestu u svojim poslovnim prostorijama.

U slučaju gubitka, krađe smart kartice ili sumnje da je došlo do povrede tajnosti kredencijala za pristup, lice na čije ime je izdata smart kartica i korisnik informacionog sistema BDD Convest dužni su da odmah o tome

obaveste Centralni registar radi blokiranja pristupa informacionom sistemu Centralnog registra za tu smart karticu.

3. Analiza aktivnosti u programima informacionog sistema centralnog registra

3.1 Definisanje predmeta analize

Definisanje predmeta analize u programima informacionog sistema centralnog registra, podrazumeva određivanje korisnika odnosno korisničkog naloga u programu, vrste aktivnosti i vremenskog opsega u okviru koga će se analizirati aktivnosti.

3.2 Utvrđivanje registrovanih podataka

Utvrđivanje karakteristika predmeta analize na osnovu registrovanih podataka u programima Informacionog sistema Centralnog registra, podrazumeva pretraživanje podataka u samom programu ili u delu baze podataka koji nije dostupan kroz korisnički interfejs i iščitavanje podataka za odgovarajućeg korisnika, aktivnost i vremenski opseg (što može biti jedan niz podataka ili više grupa podataka u zavisnosti da li je predmet jedna ili više aktivnosti). Za realizaciju ovog koraka neophodno je konsultovati stručne službe Centralnog registra, depoa i kliringa hartija od vrednosti, koji je dobavljač programa „Web aplikacija CRHoV“ i „Beoklijent“, za samu tehniku pretraživanja programa i baze podataka.

3.3 Poređenje registrovanih podataka sa stvarnim događajima

Nakon što se uz pomoć podrške utvrde podaci registrovani u samom programu informacionog sistema centralnog registra u vezi sa predmetom analize, sledi poređenje ovih podataka sa stvarnim sledom događaja. Stvarni sled događaja se u ovom slučaju utvrđuje na osnovu pisane dokumentacije za kompletno praćenje poslovanja brokerskog i dilerskog poslovanja BDD Convest a.d. Novi Sad.

3.4 Zaključak o predmetu analize

Zaključak treba da nam pruži informaciju da li predmetna aktivnost u informacionom sistemu centralnog registra (odnosno podaci registrovani u vezi ove aktivnosti) u potpunosti odgovaraju stvarnom sledu događaja. Ukoliko se utvrdi da postoje razlike između predmetne aktivnosti u informacionom sistemu (odnosno podataka registrovanih u vezi ove aktivnosti) i stvarnog sleda događaja, neophodno je utvrditi i zašto je došlo do ove razlike (da li je došlo do: greške u informacionom sistemu, ljudske greške u korišćenju informacionog sistema, zloupotrebe od strane korisnika informacionog sistema, zloupotrebe od strane tećeg lica i slično). U skladu sa utvrđenim uzrokom razlike između podataka registrovanih za predmetnu aktivnost u informacionom sistemu i stvarnog sleda događaja, neopnodno je preduzeti odgovarajuće mere da se utvrđeni nedostaci otklone.

4. Opšti postupak kontrole aktivnosti u informacionom sistemu centralnog registra

Postupak kontrole aktivnosti u informacionom sistemu centralnog registra se sastoji od sledećih koraka:

- Definisanje predmeta kontrole (jedna ili više aktivnosti u informacionom sistemu)
- Sprovođenje postupka analize predmetne aktivnosti u informacionom sistemu
- Donošenje zaključka o predmetu kontrole, koji sadrži informaciju o tome da li je predmetna aktivnosti u informacionom sistemu u skladu sa stvarnim događajima, ili ne, kao i informaciju da li je predmetna aktivnost u informacionom sistemu ugrozila sigurnost, potpunost ili tajnost podataka koji se unose u informacioni sistem.
- Utvrđivanje odgovornosti

Postupak kontrole aktivnosti u informacionom sistemu počinje jasnim definisanjem predmeta naše kontrole. Predmet kontrole može biti pojedinačna aktivnosti u informacionom sistemu ili više pojedinačnih aktivnosti, grupisanih po nekom zajedničkom činiocu (aktivnost određenog korisnika, aktivnosti svih korisnika u jednom programu u određenom vremenskom periodu i slično).
Nakon definisanja predmeta kontrole, za svaku predmetnu aktivnost u informacionom sistemu sprovodi se postupak analize opisan u dokumentu: „CONVEST-ZIS-D-12-003_Procedura_analize.doc“.
Na osnovu rezultata sprovedene analize, donosi se zaključak da li predmetna aktivnost u informacionom sistemu u potpunosti odgovara stvarnom sledu događaja, i da li je predmetna aktivnost u informacionom sistemu ugrozila sigurnost, potpunost ili tajnost podataka koji se unose u informacioni sistem. Ukoliko se utvrdi da postoje razlike između predmetne aktivnosti u informacionom sistemu (odnosno podataka registrovanih u vezi ove aktivnosti) i stvarnog sleda događaja ili da je predmetna aktivnost u informacionom sistemu ugrozila sigurnost, potpunost ili tajnost podataka koji se unose u informacioni sistem, neophodno je utvrditi i zašto je došlo do ovakvog problema (da li je došlo do: greške u informacionom sistemu, ljudske greške u korišćenju

informacionog sistema, zloupotrebe od strane korisnika informacionog sistema, zloupotrebe od strane tećeg lica i slično).

4.1. Podela tipova kontrole aktivnosti u informacionom sistemu centralnog registra

U zavisnosti od predmeta kontrole, odnosno u zavisnosti od vrste aktivnosti u informacionom sistemu, možemo razlikovati sledeće tipove kontrole:

- Kontrola korisničkih prava pristupa informacionom sistemu
- Kontrola ispravnosti unetih podataka u informacioni sistem
- Kontrola drugih aktivnosti u informacionom sistemu

Pošto smo ranije izvršili podelu informacionog sistema u odnosu na vrstu, način i mesto registracije aktivnosti u njemu, neophodno je istaći da se kontrola aktivnosti za svaki od ovih delova razlikuje samo po načinu na koji se vrši registracija i analiza aktivnosti u pojedinim delovima informacionog sistema, ali ne i po svom sadržaju i postupku. Sadržaj i postupak kontrole se razlikuje za upravo navedene tipove kontrola, pa ćemo detaljnije opisati sadržaj i postupak ove tri grupe kontrola aktivnosti u informacionom sistemu, bez obzira na koji deo informacionog sistema se odnose.
Usklađenost korisničkih prava pristupa informacionom sistemu sa korisničkim pravima definisanim u pojedinačnim ovlašćenjima za pristup informacionom sistemu je veoma važna za sigurnost, potpunost i tajnost podataka koji se unose u informacioni sistem. Stoga je neophodna redovna kontrola usklađenosti ovih prava za svakog korisnika pojedinačno. U slučaju kontrole korisničkih prava pristupa informacionom sistemu, neophodno je kontrolisati prava pristupa određenog korisnika svakom delu informacionog sistema.
Tačnost podataka unetih u informacioni sistem je veoma važna za potpunost i pouzdanost podataka unetih u informacioni sistem, i u tom smislu se mora vršiti kontrola ispravnosti unetih podataka. Ispravnost unetih podataka koji se u informacionom sistemu nalaze u elektronskom obliku se mora kontrolisati u odnosu na dokumentaciju koja postoji u nekom drugom obliku (papirnom).
Kontrola drugih aktivnosti u informacionom sistemu se odnosi na sve druge aktivnosti koje nisu direktno povezane sa izmenama prava pristupa, unosom ili izmenom podataka u informacionom sistemu. Ove aktivnosti obuhvataju korišćenje podataka, sastavljanje izveštaja na osnovu podataka iz informacionog sistema, brisanje podataka i slično. Kontrola ovih aktivnosti vrši se u skladu sa opštim postupkom za kontrolu aktivnosti u infomacionom sistemu.

4.2. Kontrola korisničkih prava pristupa informacionom sistemu centralnog registra

U slučaju kontrole korisničkih prava pristupa, predmet kontrole je trenutno stanje korisničkih prava pristupa informacionom sistemu centralnog registra za jednog ili više korisnika. Za sve radnje sprovedene korišćenjem smart kartice u informacionom sistemu centralnog registra odgovorno je lice na čije ime je kartica izdata kao i korisnik informacionog sistema . Korišćenje smart kartice od strane nekog drugog lica, osim onog na čije ime je smart kartica izdata, strogo je zabranjeno i smatra se odgovornošću lica na čije je ime kartica izdata kao i korisnika informacionog sistema.

Pošto predmet analize nije aktivnost, već trenutno stanje informacionog sistema, analiza se vrši poređem podataka (trenutnog stanja) o pravima pristupa informacionom sistemu za određenog korisnika sa ovlašćenjem za pristup informacionom sistemu (dokumentom koji je odložen u dokumentaciji u papirnom obliku). Rezultat ove analize može biti potpuno poklapanje trenutnog stanja prava pristupa sa ovlašćenjem, ili postojanje razlike. Donošenje zaključka o predmetu kontrole, koji sadrži informaciju o tome da li se trenutno stanje prava pristupa informacionom sistemu za određenog korisnika poklapa sa njegovim ovlašćenjem za pristup informacionom sistemu, ili ne. Ukoliko postoji razlika između trenutnog stanja prava pristupa informacionom sistemu za nekog korisnika i njegovih ovlašćenja za pristup informacionom sistemu, zaključak mora da sadrži i informaciju da li je ovaj korisnik, sa većim ili manjim pravima pristupa ugrozio sigurnost, potpunost ili tajnost podataka koji se unose u informacioni sistem, kao i mere za usklađivanje prava pristupa informacionom sistemu i ovlašćenja ovog korisnika.

4.3. Kontrola ispravnosti unetih podataka u informacioni sistem centralnog registra

U slučaju kontrole unetih podataka u informacioni sistem centralnog registra, predmet kontrole su uneti podaci u ovaj informacioni sistem.
Pošto predmet analize nije aktivnost, već trenutno stanje podataka unetih u informacioni sistem, analiza se vrši poređem unetih podataka (trenutnog stanja) sa pisanom dokumentacijom za kompletno praćenje brokerskog i

dilerskog poslovanja BDD Convest a.d. Novi Sad. Rezultat ove analize može biti potpuno poklapanje trenutnog stanja unetih podataka, ili postojanje razlike.
Donošenje zaključka o predmetu kontrole, koji sadrži informaciju o tome da li se podaci uneti u informacioni sistem poklapaju sa pisanom dokumentaciom za kompletno praćenje brokerskog i dilerskog poslovanja BDD Convest a.d. Novi Sad, ili ne. Ukoliko postoji razlika između podataka unetih u informacioni sistem i pisane dokumentacije za kompletno praćenje brokerskog i dilerskog poslovanja BDD Convest a.d. Novi Sad, zaključak mora da sadrži i informaciju kako je došlo do unosa pogrešnih podataka, i da li je ugrožena sigurnost, potpunost ili tajnost podataka koji se unose u informacioni sistem, kao i mere za usklađivanje podataka unetih u informacioni sistem i pisane dokumentacije za kompletno praćenje brokerskog i dilerskog poslovanja BDD Convest a.d. Novi Sad..

4.4. Kontrola drugih aktivnosti u informacionom sistemu centralnog registra

U slučaju kontrole aktivnosti u informacionom sistemu centralnog registra, predmet kontrole je jedna ili više aktivnosti u informacionom sistemu, koju je izvršio određeni korisnik.
Nakon definisanja predmeta kontrole, za svaku predmetnu aktivnost u informacionom sistemu sprovodi se postupak analize opisan u dokumentu: „CONVEST-ZIS-D-12-003_Procedura_analize.doc“.
Na osnovu rezultata sprovedene analize, donosi se zaključak da li predmetna aktivnost u informacionom sistemu u potpunosti odgovara stvarnom sledu događaja, i da li je predmetna aktivnost u informacionom sistemu ugrozila sigurnost, potpunost ili tajnost podataka koji se unose u informacioni sistem. Ukoliko se utvrdi da postoje razlike između predmetne aktivnosti u informacionom sistemu (odnosno podataka registrovanih u vezi ove aktivnosti) i stvarnog sleda događaja ili da je predmetna aktivnost u informacionom sistemu ugrozila sigurnost, potpunost ili tajnost podataka koji se unose u informacioni sistem, neophodno je utvrditi i zašto je došlo do ovakvog problema, i doneti mere za usklađivanje stanja u informacionom sistemu i stvarnog sleda događaja, odnosno dodatne mere zaštite informacionog sistema.