Coduri de practici

si proceduri al

Cert Digital – Arhivare Electronica

Referinta: 1/2015

Versiune: 1.0.2

Pagini:

Nivel de distributie: Audienta generala

EMISA DE:			
DEPARTAMENT	**NUME**	**SEMNATURA**	**DATA**
CERTDIGITAL - AE	IONICA BOGDAN		01.10.2015

APROBATA DE:			
DEPARTAMENT	**NUME**	**SEMNATURA**	**DATA**
CONDUCERE	CUSMAN ADELIN		01.10.2015

ISTORICUL MODIFICARILOR:			
VERSIUNE	**AUTOR**	**DETALII MODIFICARI**	**DATA:**
1	IONICA BOGDAN	REALIZARE PROCEDURA CERTDIGITAL - AE	04.02.2013
2	IONICA BOGDAN	ACTUALIZARE PROCEDURA CERTDIGITAL -AE	01.10.2015

Cuprins

Termeni si definitii

Acces	Posibilitatea utilizarii unei resurse informationale pe baza unui drept dobandit
Administrator	Utilizator care este autorizat de a folosi conturi administrative sau privilegiate pentru a-si indeplini sarcinile de serviciu. In general, administratorul are dreptul de gestiune asupra celorlalte tipuri de utilizatori.
Angajat	Orice persoana care are o relatie de angajament cu CertDigital in baza unui contract de munca semnat.
Audit de conformitate	Revizuire periodica efectuata asupra anumitor procese, in urma careia se stabileste gradul de conformitate cu standardele cerute
Autentificare	Validarea identitatii unui utilizator sau a unei entitati. Procesul autentificarii verifica daca entitatea este cea care pretinde a fi si in functie de rezultatul obtinut ofera sau nu acces catre resursele solicitate.
Cod de Practici si Proceduri	Document ce reglementeaza activitatea de furnizare a serviciilor de certificare
Colaborator	Orice persoana care are o relatie de angajament cu CertDigital in baza unui contract de colaborare semnat intre persoana si CertDigital sau intre CertDigital si compania pentru care lucreaza persoana respectiva
Compromitere	O incalcare a unei politici de securitate care duce la pierderea controlului asupra unei informatii cu caracter sensibil
Confidentialitate	Reprezinta un principiu de securitate care restrange accesul datelor doar la persoanele autorizate.
Control al accesului	Limitarea si verificarea accesului la sistemele informatice cu scopul de a elimina utilizarea

	neautorizata a acestora
Criptare	Transformarea textului clar in text criptat cu scopul de a ascunde continutul informatiilor pentru a preveni modificarea si utilizarea neautorizata a acestora.
Date in forma electronica	Reprezentari ale informatiei intr-o forma conventionala adecvata crearii, prelucrarii, trimiterii, primirii sau stocarii acesteia prin mijloace electronice
Entitate	Termen folosit pentru a descrie un client. De exemplu, o entitate poate fi o companie, un trust, sau o persoana fizica
Extensii	Campuri de extensie in certificatele X.509 v.3
Firewall	Reprezinta un echipament sau o serie de echipamente configurate astfel incat sa asigure filtrarea, criptarea sau intermedierea traficului intre domenii diferite de securitate pe baza unor reguli predefinite
HTTPS	Protocol de comunicare client-server similar HTTP, care permite vizualizarea de pagini web intr-un mod securizat bazat pe criptarea informaţiilor transmise de catre server şi decriptarea acesteia de catre client, folosind certificatul serverului, acceptat la iniţializarea conexiunii.
Incident de Securitate a Informatiei	Eveniment declansat accidental sau intentionat care altereaza informatiile si/sau echipamentele si care provoaca pierderea partiala sau completa a confidentialitatii/ integritatii informatiilor ori indisponibilitatea acestora.
Integritate	Principiu de securitate care asigura ca informatiile si sistemele informationale nu sunt modificate in mod accidental sau in mod voit.
Internet	Reprezinta o multitudine de calculatoare conectate intr-o retea globala care permite

	partajarea datelor (din institutii academice, institute de cercetare, companii private, agentii guvernamentale, indivizi, etc.) care pot fi accesate de la distanta
Modul de securitate hardware	Echipament hardware controlat printr-un software, care realizeaza operatii criptografice (inclusiv criptare si decriptare)
Nume distinct (ND)	Grup de informatii ale unei entitati ce alcatuiesc un nume distinctiv prin care se deosebeste de alte entitati similiare
Pagina web	Document electronic, disponibil prin Internet
PKCS#10	Sintaxa standard pentru cererile de certificat si standard de criptare a cheii publice #10, dezvoltat de catre RSA Security Inc.
Politica de Securitate a Informatiei	Politica ce sta la baza modului de abordare, de catre CertDigital, a problemelor referitoare la Managementul Securitatii Informatiilor.
Securitatea Informatiilor	Pastrarea confidentialitatii, integritatii si disponibilitatii informatiilor si asigurarea autenticitatii, responsabilitatii, nonrepudierii si acuratetii informatiei in scopul asigurarii continuitatii afacerii, minimizarii riscurilor si maximizarii profitului operational si a oportunitatilor de afaceri.
Semnatar	Persoana specificata ca subiect al certificatului ce detine cheia privata aferenta cheii publice din certificat.
Semnatura electronica	Grup de date in forma electronica atasate sau asociate logic cu alte date in forma electronica si care servesc ca metoda de identificare
Sistem de Detectie A Intruziunilor (IDS)	Sistem folosit pentru detectarea accesului neaprobat intr-o retea sau o statie de lucru.
Utilizator	Beneficiarul serviciilor de certificare, care, in baza unui contract incheiat cu un furnizor de servicii de certificare, denumit in continuare

	furnizor, deţine o pereche funcţionala cheie publica-cheie privata şi are o identitate probata printr-un certificat digital emis de acel furnizor
CD AE	Cert Digital Arhivare Electronica
TDD	Titular Drept Dispozitie = persoana fizică sau juridică proprietară sau, după caz, emitentă a documentului, care are dreptul de a stabili şi modifica regimul de acces la document, conform legislaţiei în vigoare
Administrator al arhivei electronice	Persoana fizică sau juridică acreditată de autoritatea de reglementare şi supraveghere specializată în domeniu să administreze sistemul electronic de arhivare şi documentele arhivate în cadrul arhivei electronice
Arhivă electronică	Sistemul electronic de arhivare, împreună cu totalitatea documentelor în formă electronică arhivate
Furnizor de servicii de arhivare electronică	Orice persoană fizică sau juridică, acreditată să presteze servicii legate de arhivarea electronică
Mediu de stocare	Orice mediu pe care se poate înregistra sau de pe care se poate reda un document în formă electronică
Mesaj electronic	Documentul în formă electronică ce conţine date de identificare privind expeditorul, destinatarul, precum şi momentul de timp la care acesta a fost expediat, realizat în scopul transmiterii la distanţă a unei informaţii prin mijloace electronice
Regim de acces la document	Gradul în care se acordă drept de acces la document de către titularul dreptului de dispoziţie asupra documentului
Sistem electronic de arhivare	Sistemul informatic destinat colectării, stocării, organizării şi catalogării documentelor în formă electronică în scopul conservării, consultării şi redării acestora

1. Cadrul general

1.1 Marca CertDigital

CertDigital reprezinta marca inregistrata sub egida caruia S.C. Centrul de Calcul S.A. furnizeaza serviciile de certificare, marcare temporala si arhivare electronica. De fiecare data cand in continutul acestui document se fac referiri la CertDigital, acele referiri implica compania Centrul de Calcul S.A.

1.2 Continut

Documentul „Codul de Practici si Proceduri Cert Digital AE" defineste practicile si procedurile de lucru implementate de S.C. Centrul de Calcul S.A. (de aici inainte referita ca „CertDigital") in procesul de furnizare a serviciilor de arhivare electronica operate sub denumire "Cert Digital Arhivare Electronica" (CD AE) in conformitate cu prevederile Ordinul MCSI nr. 489/ 15.06.2009 privind normele metodologice de autorizare a centrelor de date.

1.3 Sponsorul procedurii

Documentul curent se afla sub sponsorizarea Conducerii CertDigital.

1.4 Audienta si aplicabilitate

In sfera de aplicabilitate a Codului de Practici si Proceduri CD AE se include totalitatea participantilor la serviciile de arhivare electronica CertDigital, respectiv abonati, distribuitori sau alte parti contractante.

2. Politici si proceduri de lucru

2.1 Descriere generala

Cert Digital – Arhivare Electronica este sistemul de arhivare electronica al SC CENTRUL DE CALCUL SA, ce vine ca o completare fireasca a serviciilor de furnizare certificate calificate si marcare temporala oferite clientilor.

Cert Digital – Arhivare Electronica este un sistem construit dupa toate reglementarile legale in vigoare si ofera posibilitatea de a pastra documente in forma electronica pe o perioada de timp stabilita de titularul documentului, cu scopul conservarii, consultarii si editarii acestuia. Documentele arhivate electronic pot fi documente create in forma electronica, sau copii electronice ale unor documente create pe suport hartie, si apoi semnate electronic.

Accesul la documentele arhivate in sistemul Cert Digital – Arhivare Electronica este permis doar utilizatorilor autorizati de SC Centrul de Calcul SA sau de proprietarul documentelor arhivate, identificati prin: utilizator si parola (furnizate de Cert Digital – Arhivare Electronica la momentul configurarii utilizatorilor), certificat digital valid (obtinut de la un furnizor acreditat de semnatura electronica).

Regimul de acces la un document în formă electronică, precum şi modificarea acestuia se stabilesc exclusiv de către titularul dreptului de dispoziţie asupra documentului printr-un act, care va fi semnat atât de titularul dreptului de dispoziţie asupra documentului, cât şi de administratorul Cert Digital – Arhivare Electronica. Regimul de acces la documentul în formă electronică, va fi înscris în fişa de format electronic a documentului, iar actul prin care s-a stabilit acest regim, generat electronic sau transferat în format electronic, va constitui o anexă a documentului arhivat.

Actiunile permise utilizatorilor (introducere, cautare, editare, modificare, stergere, vizualizare, descarcare, printare) vor putea fi definite pentru fiecare utilizator in parte in profilul acestuia. La nivelul portalului exista o sectiune de administrare ce pemite

configurarea actiunilor permise fiecarui utilizator, inclusiv definirea utilizatorului cu rolul TDD.

In Cert Digital – Arhivare Electronica nu se arhiveaza documente care contin informatii cu regim de acces public sau informatii clasificate in sensul Legii nr. 182/2002 privind protectia informatiilor clasificate.

2.2 Infrastructura tehnica

SC Centrul de Calcul SA dispune de doua centre de date, denumite in continuare Sediul Primar si Sediul Secundar. Sediul Secundar este amplasat într-o locatie diferită ca poziţie geografică faţă de Sediul Primar şi este protejat prin aceleaşi măsuri de securitate ca şi Sediul Primar.
Sediul Secundar este echipat şi configurat cu hardware capabil să preia toate serviciile sub marca CertDigital, replicarea în timp real a datelor din Sediul Principal facând posibilă furnizarea serviciilor deservite din punctul în care şi-a încetat activitatea Sediul Primar, în cel mai scurt timp posibil.

Cele doua centre de date sunt realizate astfel incat sa raspunda tuturor cerintelor de siguranta si securitate:

- centrele de date dispun de sisteme de climatizare care să asigure valori optime de temperatură şi umiditate în vederea funcţionării echipamentelor în condiţii de siguranţă

- centrele de date dispun de sisteme de prevenire si stingere a incendiilor (sisteme de alarmă în caz de incendiu, extinctoare, senzori fum) pentru evitarea deteriorarii echipamentelor

- reteaua electrica este dimensionata astfel incat sa suporte un consum cu 10-15% mai mare decat nivelul maxim de consum pe care l-ar putea atinge echipamentele existente; este protejata impotriva varfurilor de tensiune prin echipamente de tip diferential

- garantarea siguranţei la defecţiunile previzibile ale sistemelor de utilităţi (apă, gaze etc.) care deservesc spaţiile care găzduiesc centrele de date este asigurata prin faptul ca nu exista racorduri la utilitati in interiorul centrelor de date si nici in apropierea acestora; de asemenea exista personal administrativ cu atributii privind asigurarea si monitorizarea bunei functionari a instalatiilor si echipamentelor care deservesc centrele de date

- centrele de date dispun de dispozitive UPS care să asigure funcţionarea neîntreruptă a echipamentelor în cazul opririi alimentării cu curent electric de la reţeaua principală; Sediul Primar dispune in plus si de generator de curent.

- reteaua electrica care deserveste fiecare centru de date asigura duplicarea elementelor retelei, permitand comutarea si cuplarea automata la sursa secundara de energie;

- pentru a minimiza riscul aparitiei de probleme tehnice, infrastructura centrelor de date a fost realizata plecand de la premisa asigurarii scalabilitatii si continuitatii, respectând recomandările producătorilor echipamentelor, fiind prevazut si un contract de mentenanta cu furnizorul echipamentelor.
- echipamentele critice, de a căror funcţionare permanentă depinde continuitatea funcţionării centrului de date (router, switch, etc) sunt dublate de echipamente de rezervă, care asigura continuitatea functionarii centrelor de date pe parcursul operaţiunilor de mentenanţă ce implică oprirea sau deconectarea unui echipament critic şi/sau pe perioada în care echipamentul principal este afectat de defecţiuni tehnice.

- pentru asigurarea securitatii fizice a echipamentelor din centrul de date se porneste de la principiul ca toate drepturile sunt in general restrictionate in cazul in care nu exista o aprobare sau o autorizare explicita in conformitate cu politicile si procedurile CertDigital – Arhivare Electronica.

  De asemenea sunt prevazute urmatoarele masuri de securitate, atat pentru Sediul Primar cat si pentru Sediul Secundar:
  - Sediul centrului de date este dotat cu sistem de alarma si control acces (DVR stand-alone, camere de supraveghere, control acces, cititor de proximitate, senzori de miscare, fum, alarme).
  - SC Centrul de Calcul SA are incheiat un contract cu firma specializata de securitate care asigura intervenţia unui echipaj in maxim 6 minute de la receptionarea semnalelor antiefractie, antiincendiu sau panica.
  - Camera unde se gasesc echipamentele este protejata suplimentar cu o uşa metalica antiefractie, accesul realizându-se pe baza unei cartele magnetice, prin introducerea unui cod de securitate si actionarea unei chei, dispozitive pe care doar administratorul sistemului şi Directorul General le pot actiona.

In cadrul procesului de control al accesului fizic, sunt definite reguli si nivele diferite de acces pentru personalul care deserveste Sediul Primar si Sediul Secundar. Pentru asigurarea securităţii accesului prin mijloace electronice la documentele arhivate, infrastructura IT CertDigital AE beneficiaza de sisteme de protectie atat la nivel intern cat si la nivel extern prin folosirea unor:

- sisteme de detectie a intruziunilor
- solutii de firewall
- sisteme antivirus
- definirea de reguli si nivele de acces la informatiile solutiei de arhivare electronica; accesul utilizatorilor in sistemele CertDigital AE este permis direct doar pentru procesele care au o stransa legatura cu activitatea pe care o desfasoara
- jurnalizarea automată a acţiunilor efectuate în sistem

Managementul infrastructurii IT din cadrul Sediului Primar si Sediului Secundar este asigurat prin utilizarea platformei SpiceWorks si AdminDashBoard (platforma proprie) .

Functionarea centrelor de date asigura:

- jurnalizarea cronologică a acţiunilor efectuate în toate componentele sistemului, atat cele hardware cat si cele de natura software .
- evaluarea la intervale regulate a infrastructurii centrului de date, a sistemului de securitate, a echipamentelor folosite, inclusiv a sistemelor de backup se realizeaza prin:
    - monitorizarea zilnica a infrastructurii, sistemelor si echipamentelor din centrele de date;
    - analiza riscurilor care pot influenta CertDigital AE
    - efectuarea la intervale determinate a procedurilor de mentenanta
    - evaluarea la intervale determinate a nivelelor de performanta a serviciilor oferite;
- utilizarea sistemelor de management al calitatii ISO 9001, ISO 27001
- evaluarea efectelor extinderilor si upgrade—urilor se realizeaza prin monitorizarea continua a capacitatii resurselor infrastructurii tehnice, analiza posibilitatilor de extindere/upgrade, analiza riscurilor si consecintelor implicate de aceste extinderi, si testarea posibiltatilor de extindere/upgrade intr-un mediu de testare, care sa nu afecteze functionarea centrelor de date
- realizarea auditului regulat al procedurii de politica si securitate.

2.3 Echipamente si software

1. HSM: SafeNet Cavium K4 CN1010-350-NFB-1.0-G Cryptographic Module VBD-03-0200

2. Servere (2 bucati):

- Model:Fujitsu RX200 S6
- Procesor: 2 x Intel Xeon E5620 4C/8T 2.40 GHz 12 MB, VT/DBS/Turbo-Boost
- Memorie: 64GB registered ECC DDR3
- Hard disk drive: 2x 500GB 7.2k hotplug
- Sistem Operare : Linux

3. Network Storage System:

- Host Server:
  - Procesor: 1x Intel Xeon Quad Core 2.33Ghz E5345 CPU
  - RAM: 8GB RAM
  - HDD: 73GB 2.5" SAS Drive Room for 1 more Drive (Tray not included)
  - Raid Controller Card: LSI Mega RAID MR SAS 8888ELP RAID Controller Card
  - Placa de baza: Intel S5000PSL
  - Modul Rackable Systems Roamer IP LTRX xPort
  - Sursa alimentare: 450W

- Expander(2 bucati):
  - Rackable Systems Omnistor SE3016
  - 16 bay-uri per expander compatibile SAS/SATA

4. IDS:

- Max users: 50
- Interfaces: 4x10/100/1000 Mbps
- Throughput (Firewall): 100 Mbps

5. Router –DELL SonicWALL, 2WAN+3LAN Load balance Router (1 buc):

- Porturi: 5
- Standarde:Supports Layer 4 Bandwidth Management
- Gigabit Ethernet WAN and LAN ports
- Altele:Supports Virtual Server / DMZ / Access Control
  Supports VPN pass through / VPN Failover /SSL VPN
  Built in DNS Server and Auto Backup Connection
- Protocoale suportate:Supports Inbound and Outbound Load Balancing by Bytes Packet and Session

6. UPS APC Smart UPS 1000VA 670W 2U line interactive (4 buc):

- Putere (VA):1000
- Tensiune de alimentare (V):230V

7. Switch D-LINK DGS-1210- 24 Port (4 buc):

- Porturi: 24
- Standarde: 802.3af
  802.3at
- Cu management: DA
- Management: SNTP , MON v1, ICMPv6, SNMP Trap,TFTP Client,Telnet Serve,Simplified CLI,BootP/DHCP Client,IPv4/v6 Dual Stack,SmartConsole Utility,Configurable MDI/MDIX,DHCP Auto Configuration,IPv6 Neighbor Discovery,Multi-Language Web-based GUI, SNMP Supports v1, v2, v3, Altele: QoS with Four Priority Queues, Port Mirroring, Q-in-Q VLAN for performance and security, 2 Dual Media for Flexible Fiber Connection,
  Rack mountable, Ventilation : 2 fans
- Alimentare (V/Hz): 10 to 240 VAC, 50/60HZ internal universal power supply
- Putere consumata (W): 9.7W / 120W

2.4 Solutia de arhivare electronica

Solutia Cert Digital Arhivare Electronica permite arhivarea electronica a documentelor incarcate manual sau automat, conform Legii 135/2007.
Cert Digital Arhivare Electronica este alcatuita din urmatoarele componenete:
1. Modul client — Interfata web ce permite accesarea documentelor stocate in Arhiva Electronica, introducerea de documente noi , definire TDD si utilizatori cont client.
2. Modul administrare – Interfata web accesibila de catre operatorii ce deservesc centrul de date, ce permite corectarea meta-datelor documentelor inainte de a fi primite in arhiva, operatii aferente primirii documentelor in arhiva, configurarea modulelor, generare rapoarte si auditare actiuni.
3. Modul interfatare agenti - Componenta ce asigura conectivitatea cu aplicatii de tip agent ce pot fi configurate sa introduca automat date in arhiva electronica prin procedeul de sincornizare cu arhiva locala a clientului.
4. Componenta de stocare — Asigura si gestioneaza operatiuniile de salvare a documentelor si a meta-datelor aferente.
Toate aceste componente interactioneaza intre ele, permitand functionarea optima a Cert Digital Arhivare Electronica si a tuturor operatiunilor pe care le presupune: accesul la aplicatie, introducerea metadatelor si a documentelor aferente manual/ automat, generarea de rapoarte, sectiunea de administrare a aplicatiei, istoricul actiunilor efectuate in sistem.

Pentru a asigura functionarea optima a Cert Digital Arhivare Electronica, infrastructura IT necesara sistemului informatic a fost realizata avand in vedere:

- o solutie IT redundanta atat in Sediul Primar cat si in Sediul Secundar, pentru a asigura minimizarea timpului de intreruperie a serviciului de arhivare electronica in cazul in care unul sau mai multe sisteme critice ale sistemului principal sunt intrerupte ca urmare a unor evenimente neprevazute (ex. dezastru natural)
- stocarea informatiilor pe solutii de stocare redundante
- regasirea informatiilor se realizaeaza tinand cont de regulile stabilite in sectiunea de administrare

3. Practici si proceduri operationale in domeniul IT

3.1 Procedura de control al accesului fizic

Regulile pe care se bazeaza masurile de control al accesului pornesc de la principiul ca toate drepturile sunt in general restrictionate in cazul in care nu exista o aprobare sau o autorizare explicita in conformitate cu politicile si procedurile CertDigital.

3.1.1 Amplasarea locatiei

Sediul CertDigital este localizat in str. Tudor Vladimirescu, nr. 17, Targu-Jiu, judetul Gorj.

3.1.2 Protectie impotriva accesului neautorizat

Centrul de date ce deserveste Cert Digital – Arhivare Electronica este dotat cu sistem de alarma si control acces (DVR stand-alone, camere de supraveghere, control acces, cititor de proximitate, senzori de miscare, fum, alarme).
CertDigital are incheiat un contract cu firma specializata de securitate care asigura intervenţia unui echipaj in maxim 6 minute de la receptionarea semnalelor antiefractie, antiincendiu sau panica.
Camera unde se gasesc echipamentele centrului de date este protejata suplimentar cu o uşa metalica antiefractie, accesul realizându-se pe baza unei cartele magnetice, prin introducerea unui cod de securitate si actionarea unei chei, dispozitive pe care doar administratorul sistemului şi Directorul General le pot actiona.

3.1.3 Accesul fizic

Conducerea CertDigital indentifica drepturile de acces necesare angajatilor si comunica aceste drepturi personalului responsabil pentru a fi implementate in conformitate cu procedurile in vigoare.
Accesul in incinta sediului se face pe baza urmatoarelor reguli:

- Fiecare angajat CertDigital are implicit acces deplin la biroul sau;
- Pe toata durata de desfasurare a programului, fiecare angajat are acces in toate zonele, cu exceptia zonelor pe care managerul responsabil le-a marcat ca zone cu acces limitat;
- Dreptul de acces pentru colaboratori, consultanti, personal responsabil de curatenie etc. este permis numai in zonele in care isi desfasoara activitatea. Accesul se va face prin specificarea locului si a timpului necesar si va fi aprobat de catre managerul responsabil;

- Vizitatorilor le este permis accesul doar in spatiile de receptie, iar accesul in zonele securizate se va face numai in baza unei nevoi definite clar pentru desfasurarea activitatii si in permanenta supraveghere a unui angajat CertDigital;
- Personalul IT emite recomandari privind regulile de acces pentru consultantii si colaboratorii fiecarui departament care au o relatie de afaceri cu tertii.

3.1.4 Controale de mediu in zonele IT critice

Pentru stabilirea conditiilor optime in zonele IT critice au fost implementate urmatoarele masuri:

- Sisteme de aer conditionat si ventilatoare montate pe rack-uri care asigura o temperatura optima de functionare a echipamentelor IT;
- Echipamente de tip UPS ce deservesc toate dispozitivele hardware cu rol critic in furnizarea serviciilor de arhivare electronica : storage, servere, HSM-ul, router-ul, firewall-ul, switch-urile şi modem-urile de internet;
- Conexiune la o retea electrica separata pentru a asigura protectia impotriva supratensiunii;
- Pentru evitarea unor posibile amenintari, echipamentele sunt aşezate intr-un rack inaltat, care este protejat printr-o incuietoare cu cheie.
- Sisteme de detectie a fumului si sisteme de stingere a incendiilor.

3.2 Politica de securitate

Masurile de securitate implementate de CertDigital care asigura desfasurarea activitatii de arhivare electronica in conditii optime se impart in:

- masuri de asigurare a redundantei pentru datele critice;
- masuri de asigurare a continuitatii serviciilor oferite;
- masuri de protectie fata de greselile personalului angajat;

3.2.1 Masuri de asigurare a redundantei pentru datele critice

Sistem de mirroring pentru hard-disk-urile serverelor :siguranţa datelor este asigurata de sisteme ce se bazeaza pe matrici RAID Mirroring forma duplicarea datelor asigurand protecţie impotriva pierderii fizice a informaţiilor.

Sistem de clustering pentru serviciul de arhivare electronica: server-ul ce gazduieste serviciul de arhivare electronica este setat sa lucreze in clustering cu alt server de rezerva, asigurându-se astfel un nivel ridicat de disponibilitate a serviciilor.
Proces de backup sistematic: datele aferente serviciului de arhivare electronica sunt salvate şi arhivate periodic in conformitate cu prevederile procedurii de salvare si restaure a datelor.

3.2.2 Masuri de asigurare a continuitatii serviciilor oferite

In vederea asigurarii unei continuitati a serviciilor oferite, CD AE dispune de conexiune la Internet prin doua linii oferite de furnizori diferiti, dupa cum urmeaza:

- RDS – linie principala fibra optica de 150 MB garantat;
- Telekom – linie back-up fibra optica de 50 MB garantat.

3.2.3 Masuri de protectie fata de greselile personalului angajat

Personalul angajat al CD AE este format din oameni calificaţi cu o bogata experienţa profesionala şi care poseda certificari şi diplome.
Personalul implicat in procesele CD AE trebuie sa prezinte dovada indeplinirii cerinţelor legate de trecut, calificari şi experienţa, necesare pentru a indeplini in mod competent şi satisfacator responsabilitaţile postului respectiv.
Activitaţile sunt imparţite pe baza de roluri conform fişei de responsabilitaţi, astfel incât o activitate mai complexa sa poata fi dusa la capat numai cu acordul mai multor persoane. Mai mult decat atât, pentru activitaţi critice este necesar acordul scris al Directorului General.

3.3 Procedura de salvare si restaurare a datelor

Programul de salvare a datelor este dezvoltat in baza unei evaluari a riscului efectuate de catre personalul IT din cadrul CertDigital AE.
Administratorul de sistem este responsabil de intregul proces de back-up si restaurare, care trebuie sa se desfaşoare conform curentei proceduri. Pentru procedura de restuarare este necesara, insa, o imputernicire scrisa, semnata de Conducerea CertDigital.

3.3.1 Procesul de backup/salvare

La nivelul Cert Digital – Arhivare Electronica, sunt identificate doua seturi de date critice:

- baza de date SQL Server, unde se pastreaza informatiile despre TDD, fisa electronica a documentelor, utilizatori, drepturi etc

- fisierele de tip arhiva ce contin documentele intrate in arhiva electronica

Procesul de backup se realizeaza de catre adminsitratorul de sistem, care include ambele puncte de la paragraful de mai sus.
Procesul de back-up al bazei de date SQL Server se executa automat, programatic, folosind programe (scripturi de back-up) native SQL Server in urmatoarele etape:

1. Full Back-up (Salvare Totala) - se executa saptamânal in fiecare zi de vineri la ora 23.00. Backup-ul consta in salvarea in intregime a bazei de date: tabele, structura, vederi, proceduri stocate si functii, indecsi, rezultand o copie exacta a bazei de date initiale la momentul salvarii. Salvare se efectueaza pe Network Storage intr-un fisier denumit “ae_full_backup.bak”.
2. Differential Back-up (Salvare Diferentiala) se executa automat zilnic, o singura data, la orele 1.00 si consta in salvarea tuturor modificarilor din baza de date care au avut loc de la ultimul Full Backup. Salvare se efectueaza pe Network Storage intr-un fisier denumit ae_diff_backup.bak.
3. Transaction Log Back-up (Salvarea Jurnalului de Tranzactii) se executa automat zilnic, incepând cu ora 8:00 pâna la ora 18:00, din doua in doua ore, incluzând intervalele orare. Prin aceasta procedura se salveaza jurnalul operatiunilor efectuate asupra bazei de date de SQL. Salvare se efectueaza pe Network Storage intr-un fisier denumit “ae_log_backup.bak”.

In fiecare saptamâna in ziua de Vineri, salvarile efectuate pe Network Storage, atât aferente bazei de date SQL cât si fisierele de tip arhiva, sunt scrise pe suport magnetic CD/DVD, pe care se va nota data si ora la care au fost salvate. Ulterior unitatile de tip CD/DVD sunt pastrare intr-un loc sigur, in fisete de metal protejate de cheie si de sistemul de securitate dedicat, din incinta.

Intre Sediul Principal si Sediul Secundar exista implementate proceduri de sincronizare, astfel ca totate datele din Sediul Principal sa fie disponibile locatiei secundare in cazul necesitatii activarii Sediului Secundar.
In fiecare saptamâna in ziua de Vineri, salvarile efectuate pe Network Storage, sunt scrise pe suport magnetic CD/DVD, pe care se va nota data si ora la care au fost salvate. Ulterior unitatile de tip CD/DVD sunt pastrare intr-un loc sigur, in fisete de metal protejate de cheie si de sistemul de securitate dedicat, din incinta CertDigital.

3.3.2 Procedura de restaurare

Implementarea procedurilor de restaurare se desfasoara dupa cum urmeaza:

- Pentru ca restaurarea completa sa poata fi realizata in orice moment se pastreaza copii ale discurilor de instalare a sistemelor de operare, a aplicatiilor care compun sistemul informatic de arhivare, a serverului Web, a SGBD-urilor
- Departamentul IT realizeaza cel putin trimestrial testarea mediului de back-up pentru a verifica faptul ca acesta poate fi folosit pentru restaurarea datelor.
- Testarea restaurarii – se realizeaza pe mediul de test si are ca scop verificarea functionarii corecte a datelor restaurate.

In cazul identificarii unor defecţiuni hardware (defectare a placii de baza, defectare a unitaţii de stocare sau altele) se trece la remedierea problemei prin inlocuirea componentelor defecte cu alte componente noi compatibile având caracteristicile tehnice identice cu cele ale componentelor iniţiale.
Dupa instalarea noilor componente in sistem, daca este necesar, se va trece la repopularea cu datele existente salvate inainte de apariţia problemei. Pentru executarea procedurii de restaurare a datelor de pe suportul de back-up (CD sau DVD) este necesar acordul scris al Directorului General.
Procesul de restaurare se va realiza de catre administratorul de sistem sub supravegherea Directorului Tehnic, care va raspunde de acest proces.

3.4 Procedura de administrare a conturilor in sistemele CertDigital Arhivare Electronica

3.4.1 Crearea conturilor de utilizatori

Definirea conturilor de utilizatori pentru reteaua de calculatoare, sistemele informatice sau sistemele de posta electronica din cadrul CertDigital se realizeaza de catre personalul de administrare a aplicatiilor din cadrul Departamentului IT.
La angajarea unei persoane noi in cadrul CertDigital care are nevoie de acces intr-unul sau mai multe dintre sistemele informatice, se va solicita de catre seful direct crearea conturilor

de utilizator necesare prin completarea unui formular pentru crearea unui cont de utilizator. In cadrul formularului se vor detalia aplicatiile si sistemele pentru care se solicita contul de acces precum si drepturile si profilele de utilizator de care respectiva persoana are nevoie pentru indeplinirea responsabilitatilor care i-au fost alocate.
Formularul completat trebuie semnat atat de catre utilizator cat si de catre superiorul direct si trebuie transmis Departamentului IT pentru implementare.
Pe baza formularului completat si a aprobarii sale, Departamentul IT va crea conturile solicitate intocmai cu drepturile si profilele specificate.

3.4.2 Modificarea conturilor de utilizatori

In cazul in care este nevoie de a modifica un cont de acces in sistemele informatice CertDigital, utilizatorul solicitant va completa un formular de modificare a unui cont de utilizator prin specificarea in detaliu a noilor drepturi pe care le solicita (aplicatii si sisteme informatice, profil de utilizator etc.) dar si a drepturilor pe care le detine si care trebuie anulate odata cu modificarea pozitiei in cadrul CertDigital.
Formularul completat este aprobat de catre superiorul direct al angajatului care isi va exprima acordul si va revizui unde este cazul detaliile privind conturile de utilizator solicitate, dar si a celor care vor fi anulate.
Pe baza formularului completat si a aprobarii sale, Departamentul IT va executa operatiile de modificare a conturile in conformitate cu detaliile specificate.
De asemenea, in cazul intreruperii activitatii pentru o perioada mai lunga de 60 de zile (de exemplu in cazul unui concediu de maternitate), angajatul respectiv are obligatia de a solicita prin formularul pentru modificarea unui cont de utilizator dezactivarea temporara a contului de utilizator. Formularul trebuie semnat de catre superiorul direct si trimis Departamentului IT care va actiona in consecinta.

3.4.3 Dezactivarea conturilor de utilizatori

Procesul de dezactivare a unui cont de utilizator se realizeaza pe baza fisei de lichidare emise de catre Departamentul de Resurse Umane. Astfel, in momentul terminarii contractului de munca cu CertDigital, angajatul respectiv va prezenta Departamentului IT fisa de lichidare care va contine o referire la dezactivarea conturilor sale de utilizator. Departamentul IT va dezactiva conturile imediat sau in cel mai scurt timp posibil in vederea diminuarii riscului de mentinere a unui cont activ in mod necorespunzator si va confirma acest lucru prin semnarea fisei de lichidare.

Pentru a facilita trasabilitatea activitatilor efectuate cu ajutorul conturilor de utilizator, aceastea vor fi dezactivate si nu sterse. Dupa trecerea unei perioade de minim 24 de luni de la dezactivare, Departamentul IT poate decide stergerea definitiva a conturilor.

3.5 Procedura de administrare a utilizatorilor cu drepturi privilegiate

Un drept privilegiat reprezinta accesul nerestrictionat de controalele implementate al unui utilizator la una sau mai multe functionalitati din cadrul unui sistem informatic.
Aceste drepturi includ, dar nu se limiteaza la:

- Un utilizator cu drepturi de administrator;
- Dreptul de a accesa direct bazele de date ale aplicaţiilor;
- Drept de acces pe facilitati de sistem specifice (aplicaţii, utilitare).

Alocarea drepturilor privilegiate pentru utilizatori in aplicatiile informatice din cadrul Companiei este permis decât in baza unei autorizatii si a unei nevoi justificate in fişa postului in cazul angajatilor, respectiv in contractele de servicii/ colaborare in cazul terţelor parţi.
Beneficiarii drepturilor privilegiate sunt, in general, administratorii de sisteme, administratorii de reţea, inginerii de sistem sau consultanţii din partea unor terţe parţi care necesita acces in aplicatiile informatice din cadrul CertDigital pentru a intreprinde actiuni specifice (precum intreţinere, mentenanţa, debugging etc.).
Drepturile privilegiate sunt identificate pentru fiecare element al infrastructurii (de exemplu sistem de operare, baza de date, etc.) şi pentru fiecare aplicatie. De asemenea, sunt identificate si categoriile de utilizatori pentru care vor fi alocate aceste drepturi.
Anumite situatii de urgenta pot justifica folosirea conturilor privilegiate. Astfel, este efectuata o configurare prealabila a accesului cu drepturi privilegiate si impunerea unui control adecvat. Spre exemplu, datele de acces ale conturilor de utilizatori pot fi pastrate intr-un plic sigilat intr-o locaţie sigura, alaturi de o lista cu persoane autorizate sa foloseasca in caz de necesitate aceste conturi. De asemenea, in plicul sigilat sunt incluse si datele de contact ale administratorului de sistem care trebuie contactat atunci când este necesara deschiderea plicului.

3.5.1 Administrarea conturilor de utilizatori cu drepturi privilegiate

Personalul de administrare a aplicatiilor are in responsabilitate crearea, modificarea si ştergerea conturilor de utilizatori cu drepturi privilegiate. Procesul de creare a unui cont cu drepturi privilegiate pe baza unei cereri emise implica, in plus fata de procesul obisnuit si descris in procedura de administrare a conturilor in sistemele CertDigital.

Conturile de utilizatori privilegiate trebuie permanent revizuite de catre Responsabilul de Securitate pentru a preintâmpina situatia in care ar putea exista in sistem conturi active nefolosite sau drepturi de acces acordate necorespunzator.
Personalul de administrare a sistemului, daca este posibil, nu trebuie sa foloseasca conturile cu drepturi privilegiate pentru desfasurarea activitatilor zilnice de nivel scazut. Pentru aceste activitati, fiecare administrator trebuie sa detina in paralel un cont cu drepturi normale de acces.

3.5.2 Monitorizarea conturilor de utilizatori cu drepturi privilegiate

Toate activitaţile desfaşurate prin intermediul unor conturi de utilizator cu drepturi privilegiate vor fi monitorizate si inregistrate. Conform politicii de retentie, aceste fisiere vor fi salvate şi pastrate pentru o perioada determinata de timp şi vor fi revizuite periodic sau ori de câte ori este nevoie de catre Responsabilul de Securitate. Acesta va intocmi rapoarte regulate conţinând rezultatele procesului de revizuire.

3.6 Procedura de management al parolelor pentru personalul CertDigital

Scopul acestei proceduri este de a stabili standarde de creare a parolelor, de protectie si de schimbare frecventa a acestora, astfel incat sistemul informatic CertDigital sa fie protejat impotriva accesului neautorizat.
Parolele sunt asociate cu conturile de utilizator si sunt folosite in cadrul aplicatiilor sau diverselor sisteme CertDigital (de ex. pentru acces la retea, e-mail etc.). De aceea, este necesar ca toti angajatii sa cunoasca recomandarile cu privire la alegerea unor parole adecvate.

3.6.1 Reguli privind alegerea parolelor

Parolele **adecvate** au urmatoarele caracteristici:

- Contin atat majuscule cat si litere mici (a-z, A-Z);
- Contin cifre si cel putin un caracter alfanumeric (0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./);
- Nu sunt cuvinte intalnite in nicio limba, dialect, argou, jargon etc;
- Nu se bazeaza pe informatii personale precum nume, numere de telefon etc;
- Nu coincid si nu contin numele de utilizator;
- Au lungimea minima de opt caractere.

Parolele **neadecvate** reprezinta parole cu grad scazut de complexitate ce sunt deseori caracterizate de una dintre urmatoarele specificatii:

- Reprezinta un cuvant folosit in mod uzual, cum ar fi:

- Cuvintele „CertDigital”, “Bucuresti”, “parola” sau alte derivate;
- Numele utilizatorului familie, al copiilor, colegilor de serviciu, animalelor de companie, etc.;
- Zile de nastere, adrese, numere de telefon, numarul de la masina sau alte informatii personale;
- Cuvinte sau succesiuni de litere sau cifre de genul: abcdef, 123456, zyxwvuts, 123321 etc.;
- Oricare dintre cuvintele de mai sus scrise in ordine inversa;

- Au in alcatuire cuvinte ce se regasesc intr-un dictionar (Roman, Englez etc);
- Coincid sau contin numele de utilizator;
- Au lungimea mai mica de opt caractere.

3.6.2 Protejarea parolelor de catre utilizatori

Parolele asociate conturilor de utilizatori nu sunt folosite pentru autentificarea in sisteme externe CertDigital (de exemplu, conturi personale de e-mail, conturi pe site-uri comerciale etc.). De asemnea, parolele sunt alese in mod distinct pentru fiecare tip de aplicatie care necesita autentificare prin parola.
Toate parolele sunt clasificate ca informatii confidentiale si nu este permisa stocarea acestora in sistemele informatice sau pe un alt suport.
In cazul in care controalele referitoare la folosirea parolelor nu sunt respectate, CertDigital adopta masurile adecvate in acest sens pentru a se ajunge la conformitatea cu acestea.

3.7 Procedura de securitate a informatiilor

Pentru manipularea optima a informatiei, pentru simplificarea deciziilor privind securitatea informatiilor si pentru minimizarea costurilor legate de securitatea informatiilor CertDigital are implementata o ierarhizare a informatiei pe baza confidentialitatii. Principalul scop al acestei ierarhizari este de a furniza un proces consistent de manipulare a informatiilor, indiferent de modul in care se prezinta informatia, cui ii este adresata sau cine o are in custodie.
Fiecare angajat trebuie sa aiba acces doar la informatia necesara pentru a-si indeplini sarcinile de serviciu. Informatiile sensibile trebuie accesate doar de catre angajatii carora proprietarul aplicatiei respective le-a acordat drept de acces.
Informatiile CertDigital nu trebuie folosite in alte scopuri decat cele de business aprobate in mod oficial de catre Conducere. Folosirea neaprobata a informatiilor restrictionate este

interzisa. Politica se aplica tuturor tipurilor de informatii cadrul CertDigital. Politica se aplica tuturor partilor care intra in contact cu informatiile CertDigital, inclusiv colaboratorilor externi. Utilizatorilor nu le este permis sa efectueze nicio activitate in sistemele informatice interne ce ar putea conduce la deteriorarea imaginii CertDigital.
CertDigital foloseste trei categorii de clasificare a informatiilor detaliate in continuare.

3.7.1 Informatie Publica

Aceasta informatie este aprobata de catre Conducerea CertDigital ca fiind publica. Dezvaluirea neautorizata a informatiilor publice este admisa intrucat nu poate cauza probleme companiei CertDigital, clientilor sau partenerilor de afaceri (exemplu de informatie publica brosurile si materialele de pe pagina de internet oficiala). Pentru ca informatia sa fie clasificata ca publica trebuie sa fie etichetata ca atare sub permisiunea Proprietarului Informatiei.

3.7.2 Informatie cu utilizare Interna

Utilizarea acestor informatii este permisa in cadrul CertDigital, iar in unele situatii si in cadrul organizatiilor afiliate (partenerilor CertDigital). Dezvaluirea neautorizata a acestui tip de informatii catre persoane din afara CertDigital nu este admisa si poate cauza probleme in cadrul organizatiei, clientilor sau partenerilor de afaceri. Acest tip de informatie poate fi raspandita in interiorul CertDigital fara aprobarea in avans a Proprietarului informatiei. (exemple de informatie cu utilizare interna: numerele de telefon cadrul CertDigital si adresele casutelor de e-mail).

3.7.3 Informatie restrictionata

Reprezinta informatia cea mai sensibila si necesita monitorizare permanenta. Se incadreaza la cel mai ridicat nivel de confidentialitate. Divulgarea neautorizata a acestui tip de informatie catre angajatii carora nu le este necesara poate constitui o incalcare a legislatiei si a reglementarilor in vigoare, si poate cauza probleme organizatiei, clientilor sau partenerilor de afaceri. Proprietarul informatiei poate aproba accesul la acest tip de informatii (exemple de informatie restrictionata: planurile de fuziune si achizitie si informatiile legale protejate de confidentialitatea avocat-client).

3.8 Procedura de personal

3.8.1 Cerinţe privind trecutul, calificarile, experienţa şi acceptarea

Personalul care este nominalizat pentru a face parte din echipa care se ocupa cu emiterea/revocarea certificatelor calificate si a marcilor temporare trebuie sa prezinte dovada indeplinirii cerinţelor legate de trecut, calificari şi experienţa, necesare pentru a indeplini in mod competent şi satisfacator responsabilitaţile postului respectiv.

3.8.2 Proceduri de verificare a trecutului

CertDigital face urmatoarele verificari asupra trecutului personalului:

- Confirmarea locului de munca anterior;
- Verificarea referinţelor profesionale;
- Confirmarea celei mai inalte sau relevante instituţii de invaţamânt urmate;
- Studierea cazierului judiciar
- Cautarea rapoartelor financiare;
- Cautarea rapoartelor privind permisul de conducere;
- Cautarea rapoartelor privind asistenţa sociala;

In masura in care, oricare dintre cerinţele impuse nu poate fi satisfacuta, CertDigital va folosi o tehnica de investigaţie care este permisa de lege şi care furnizeaza informaţii asemanatoare.
Factorii implicaţi in verificarea trecutului, ce pot duce la respingerea persoanelor candidate a face parte din echipa sau la luarea de masuri impotriva celor care fac parte din echipa, includ:

- Prezentarea greşita facuta de catre candidat;
- Referinţe personale nefavorabile sau care nu inspira incredere;
- Condamnari;
- Indicii ale lipsei de responsabilitate financiara.

Rapoartele care conţin astfel de informaţii sunt evaluate de personalul de la resurse umane şi securitate, care determina cursul potrivit al acţiunii, in funcţie de tipul, importanţa şi frecvenţa comportamentului dezvaluit de verificarea trecutului. Aceste acţiuni pot include masuri care pot ajunge la incheierea rapoartelor contractuale cu persoana respectiva. Folosirea informaţiilor gasite prin verificarea trecutului pentru a intreprinde astfel de acţiuni este supusa legilor aflate in vigoare.

3.8.3 Cerinţe de pregatire

CertDigital asigura personalului pregatirea necesara pentru a indeplini in mod competent şi satisfacator responsabilitaţile funcţiei. Programele de pregatire ale CertDigital sunt realizate ţinând cont de responsabilitaţile individuale şi includ urmatoarele:

- Concepte de baza despre arhivarea electronica;
- Responsabilitaţile funcţiei;
- Politicile şi procedurile de securitate şi operaţionale CertDigital AE;
- Folosirea şi funcţionarea hardware-ului şi software-ului existent;
- Raportarea şi tratarea cazurilor de incident şi compromis;
- Procedurile de recuperare in caz de dezastru şi de continuare a activitaţii.

3.8.4 Cerinţele şi frecvenţa cursurilor de perfecţionare

CertDigital furnizeaza cursuri de perfecţionare şi de actualizare pentru personal, in masura şi cu frecvenţa care permit asigurarea menţinerii nivelului necesar pentru indeplinirea competenta şi satisfacatoare a responsabilitaţilor de serviciu. Se asigura periodic pregatire de securitate.

3.8.5 Sancţiuni pentru acţiuni neautorizate

Se iau masuri disciplinare adecvate pentru acţiunile neautorizate sau pentru alte violari ale politicilor şi procedurilor CertDigital. Acţiunile disciplinare pot include masuri care duc pâna la incheiere contractului şi sunt luate in funcţie de frecvenţa şi severitatea acţiunilor.

3.8.6 Cerinţe pentru contractarea personalului

In circumstanţe limitate, se pot folosi contractanţi sau consultanţi independenţi pentru a ocupa funcţii de incredere. Orice astfel de contractant sau consultant este menţinut dupa aceleaşi criterii funcţionale şi de securitate care se aplica şi in cazul CertDigital, care se afla intr-o poziţie asemanatoare. Contractanţii şi consultanţii independenţi care nu au desavârşit procedurile de verificare a trecutului specificate la punctul 1.2 pot accesa locaţiile securizate ale CertDigital numai daca sunt escortaţi şi supravegheaţi direct de persoane de incredere.

3.8.7 Documentaţie furnizata personalului

Personalul CertDigital implicat in funcţionarea serviciilor de arhivare electronica trebuie sa citeasca codul de practici şi proceduri şi politica de securitate interna. CertDigital ofera angajaţilor sai pregatirea necesara şi alta documentaţie necesara pentru a indeplini competent şi satisfacator responsabilitaţile funcţiei.

4. Administrarea documentului

4.1 Mecanismul de schimbare

Modificarile care pot surveni in continutul acestui document sunt determinate fie de obtinerea unor neconformitati in urma unor revizuiri ale proceselor fie din imbunatatiri periodice ale fluxurilor operationale in cadrul CertDigital.

Implementarea modificarilor actualizeaza numarul de versiune al documentului si data de emitere a Codului de Practici si Proceduri AE in functie de data la care au fost efectuate modificarile.

CertDigital isi aloca dreptul de a efecta modificari de continut (corectarea erorilor de tipar, modificarea legaturilor URL publicate, schimbari in informatiile de contact etc.) asupra reglementarilor Codului de Practici si Proceduri AE.

Revizuirile Codului de Proceduri si Practici AE fara impact sau cu un impact nesemnificativ asupra semnatarilor si partilor de incredere care utilizeaza certificatele emise de CertDigital si informatiile corespunzatoare legate de starea certificatului se pot realiza si inregistra fara a notifica utilizatorii si partile de incredere si nu implica modificarea numarului de versiune a documentului sau data de intrare in vigoare.

Odata cu sintetizarea modificarilor de implementat, Codul de Practici si Proceduri TSA intra in procedura de aprobare interna care se desfasoara pe baza unui comitet format din directorul general, directorul general adjunct si managerii departamentelor tehnice.

Responsabilitatea intretinerii Codului de Practici si Proceduri AE este alocata catre managerul departamentului care asigura furnizarea serviciilor de certificare. Aferent aprobarii, Codul de Practici si Proceduri AE este transmis Autoritatii de Reglementare si Supraveghere urmand ca in termen de 10 zile, sa fie publicat si marcat ca fiind valid.

Versiunea curenta a Codului de Practici si Proceduri TSA este datata ianuarie 2013.

4.2 Mecanismul de publicare si notificare

Documentul Codului de Practici şi Proceduri AE este disponibil in forma electronica pe site-ul CertDigital la adresa: www.certdigital.ro sau poate fi solicitat prin posta electronica la adresa sediu@centruldecalcul.ro.

Prin interfata online de afisare a informatiilor public, CertDigital pune la dispozitie doua versiuni ale documentului:

- Versiunea curenta;
- Versiunea anterioara;

Documentele de securitate considerate confidenţiale de catre CertDigital sunt inaccesibile publicului.

4.3 Procedura de aprobare a Codului de Practici si Proceduri AE

Codul de practici si proceduri actualizat este considerat a fi valid din momentul publicarii sale pe site-ul CertDigital.

Utilizatorii care nu agreaza varianta actualizata a Codului de Practici si Proceduri AE si a modificarilor aferente sunt obligati ca in termen de 15 zile de la data validarii noii versiuni, sa intocmeasca o declaratie in acest sens. In acest caz, CertDigital isi atribuie dreptul de a rezilia contractul de furnizare a serviciilor de arhivare electronica in baza acestuia. Ulterior intervalului de 15 zile de la punerea in vigoare a noii versiuni, CertDigital considera ca implicit acceptul utilizatorilor.