

# *Enthusio*<sup>™</sup> MSP:

Podrška regulativnoj usaglašenosti sa standardima

Verzija 2.01



2009

## 1. Uvod

Od kraja 1990-tih, vlade donose zakonske propise koji od kompanija traže da primenjuju strogu kontrolu nad poslovanjem. Cilj ove kontrole je da se investitorima jasno ukaže na rizike i da se krajnji korisnici zaštite od zloupotrebe ličnih podataka. U globalnoj ekonomiji koja sve više rukovodeću strukturu smatra direktno odgovornom za posledice u okviru njihovog poslovanja, kompanije moraju da budu u stanju da pokažu da se služe efektivnim procesima ili pak da se suoče sa ozbiljnim posledicama, pa čak i da rizikuju da budu podložne krivičnoj odgovornosti. Kako informacione tehnologije imaju ključnu ulogu u svetu poslovanja, IT procesi i njihova efikasna primena sada predstavljaju glavne komponente prilikom provere usaglašenosti sa standardima.

**Enthusio™ MSP** omogućava pružiocima usluga (MSP – Managed Service Provider) da povećaju svoj godišnji prihod tako što nude usluge kontrole i upravljanja koje su posebno orijentisane ka usaglašenosti sa standardima od značaja za njihove klijente.

U zavisnosti od konkretne vrste poslovanja, klijenti MSP-a će imati koristi od onih njihovih usluga koje su usmerene ka bezbednosti, privatnosti, dostupnosti i proceni rizika.

Ovaj dokument opisuje:

- osnovna zakonodavna dokumenta koja se odnose na SMB (Small Medium Business) preduzeća i kakvu ulogu pružaoци usluga mogu da imaju obezbeđujući im podršku
- kako koristiti **Enthusio™ MSP** u cilju pružanja najboljih usluga uslovljenih standardima

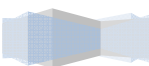
Ovaj dokument polazi od pretpostavke da ste i Vi jedan od partnera u korišćenju **Enthusio™ MSP** kome ono služi za kontrolu i upravljanje ICT okruženjem Vaših klijenata.

## 2. Kratak pregled: IT upravljanje i usaglašenost sa standardima

Vlade mnogih zemalja na međunarodnom nivou (naročito SAD, Kanada i Evropska unija) već su donele zakonske propise vezane za IT sisteme upravljanja kako bi kompanije svojim investitorima i klijentima pružile dokaz o odgovornom poslovanju. Veliki deo te odgovornosti leži upravo na onima koji upravljaju IT procesima jer informacione tehnologije obično imaju dodira sa svim aspektima poslovanja jedne kompanije.

Zakoni opisani u daljem tekstu utiču na određene vrste poslovanja, na različite načine. Neki se odnose na poslovanje svih obima; drugi samo na javna preduzeća. Neki zakoni, npr. HIPAA, pogađaju samo pojedine grane nekih oblika poslovanja, kao što je poslovanje u oblasti zdravstvene nege. Za SMB preduzeća može da bude veoma složeno i skupo da shvate kako najbolje da upravljaju IT infrastrukturom da bi poslovali u skladu sa ovim zakonima. Takođe, to može i da ih zbunjuje, jer nijedan od ovih zakona eksplicitno ne propisuje određene IT zahteve. Takođe kompanije nisu dužne da same sprovode kontrolu upravljanja kako bi funkcionisale u skladu sa zakonom, ali one mogu da budu odgovorne ukoliko nešto nije u redu.

Primenom **Enthusio™ MSP** možete svom kupcu da pomognete da prepozna kritične tačke u svojoj IT mreži koje se mogu regulisati. Korišćenjem kontrolne liste iz 4. poglavlja – *Ponuda paketa standarda sa Enthusio™ MSP* bićete u mogućnosti da nudite paket usluga za proveru usaglašenosti sa standardima, a koje se odnose na sedam glavnih zahteva u vezi sa IT, zajedničkih za većinu ovih zakonskih propisa.



### 3. Koji zakoni najviše pogađaju Vaše klijente?

Postoji niz akata koja se primenjuju na kompanije (male i velike) širom sveta. Gledano iz ugla IT, ona se uglavnom odnose na mogućnost organizacija da održavaju zadovoljavajući nivo standarda u oblasti bezbednosti i privatnosti. Nadležni za upravljanje IT sistemima moraju da obezbede raspoloživost usluga i podataka, integritet podataka i smanjenje rizika od finansijskih gubitaka usled loše primene i održavanja IT infrastrukture. U ovom odeljku dat je pregled glavnih zakonskih akata i propisa koji mogu da budu od značaja za vaše klijente.

Bez obzira na sama zakonska akta, kompanije koje se u svakodnevnom poslovanju oslanjaju na svoju infrastrukturu treba svakako da ulažu u kontrolu i održavanje svojih mreža. Mogućnosti koje pruža **Enthusio™ MSP** igraju ključnu ulogu u obezbeđivanju usaglašenosti jedne kompanije sa standardima i to na rentabilan i efikasan način.

#### **Sarbanes-Oxley (Sarbox)**

**Primena na teritoriji:** SAD/široom sveta

**Odnosi se na:** Javna preduzeća

**Opis:** Sarbanes-Oxley (Sarbox) akt donet je u SAD 2002. godine.

Ciljnu grupu ovog zakonskog akta čine sva preduzeća podložna javnoj prodaji na američkoj berzi.

Cilj ovog akta je da se obezbedi tačnost finansijskih podataka jedne kompanije i pouzdanost za to odgovornih sistema. Izazov za IT leži u upravljanju bezbednom i kontrolisanom infrastrukturom za manipulisanje podacima, procesima i istorijom podataka. Mada se ovaj akt odnosi na velika i već stabilna preduzeća, njegov visok profil imao je širom sveta veliki uticaj na postavljanje standarda pokazujući kako sve oblasti poslovanja treba da funkcionišu.

## **Gramm-Leach-Bliley (GLBA)**

**Primena na teritoriji:** SAD

**Odnosi se na:** Finansijski sektor

**Opis:** Gramm-Leach-Bliley (GLBA) je drugi američki akt iz 1999. godine.

Odnosi se na sve američke finansijske institucije, velike i male, a cilj mu je obezbeđivanje integriteta finansijskih podataka i podataka o klijentu. Uloga IT sektora je da primenjuje sisteme bezbednosti i autorizovanog pristupa i da postavlja sredstva zaštite protiv upada i rizika. Ovaj tip usklađenosti sa standardima važan je za mnoge male pružaoce finansijskih usluga koji svoj uspeh baziraju na ugovorima o pružanju usluga. Slični zahtevi na svetskom nivou mogu da se nađu u dokumentu *The New Capital Accord* (Basel II) 1998/2005.

## **Basel II**

**Primena na teritoriji:** Širom sveta

**Odnosi se na:** Finansijski sektor

**Opis:** Međunarodni ekvivalent američkom zakonskom aktu *Gramm-Leach-Bliley (GLBA)*

## **USAPATRIOT Akt, 2001, ili "Patriot Act"**

**Primena na teritoriji:** SAD

**Odnosi se na:** Fizička lica i ustanove

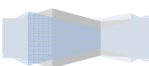
**Opis:** USAPATRIOT Akt (USAPATRIOT) iz 2001. Odnosi se na sve američke kompanije i nastoji da spreči podršku i finansiranje terorista. Takođe, cilj mu je da spreči izvoz specifične IT opreme posebne namene u određena međunarodna područja.

## **Federal Food & Drug (21- CFR-11) - Federalni akt o hrani i lekovima**

**Primena na teritoriji:** SAD

**Odnosi se na:** Zdravstveni sektor

**Opis:** Ovaj zakon odnosi se na sve kompanije čiji se rad zasniva na propisima o hrani i lekovima (u Americi FDA). Cilj ovog akta je bezbednost, integritet i raspoloživost podataka. To je naročito bitno u zdravstvenom sektoru koji se oslanja na preciznost podataka o pacijentima i proizvodima.



## *European Union Data Protection Directive*

### *(Direktiva Evropske unije o zaštiti podataka)*

**Primena na teritoriji:** Evropske unije

**Odnosi se na:** Sve oblasti poslovanja

**Opis:** Akt EUDPD (Direktiva Evropske unije o zaštiti podataka) reguliše širu kategoriju tzv. "ličnih podataka" što podrazumeva "bilo kakve podatke u vezi sa nekom osobom sa utvrđenim ili mogućim identitetom" (nosilac podataka).

## *Payment Card Industry Data Security Standard (PCI-DSS)*

### *(Standard o zaštiti podataka u industriji platnih kartica)*

**Primena na teritoriji:** Širom sveta

**Odnosi se na:** Dilere kreditnih kartica

**Opis:** Donet je 2004. godine od strane vodećih kompanija za izdavanje kreditnih kartica koje su želele da budu sigurne da će se njihovi dileri pridržavati specifičnih mrežnih standarda u cilju zaštite samog sistema kreditnih kartica kao i vlasnika kartica od moguće zloupotrebe. Ovaj standard odnosi se na sve ustanove koje izdaju platne kartice i ima pet osnovnih ciljeva: izgradnju i održavanje bezbedne mreže; zaštitu transakcionih podataka; zaštitu od zloupotrebe; primenu strogih mera kontrole pristupa i redovnu kontrolu i testiranje mreža.

## *Notification of Risk to Personal Data Act (NORPDA – US 200)*

### *(Akt o obaveštavanju o ugroženosti ličnih podataka)*

**Primena na teritoriji:** SAD

**Odnosi se na:** Sve američke kompanije i građane

**Opis:** Cilj ovog propisa je da se građanima garantuje da će ih agencije obavestiti u slučaju da su njihovi lični podaci negde dobijeni neovlašćenim putem. Zahtev za IT je da obezbedi pouzdane sisteme bezbednosti i dojavljivanja. Između ostalih, tu je i Evropska direktiva o zaštiti podataka iz 1995.

## ***Health Information Portability & Accountability Act (HIPAA)***

### ***(Akt o prenosivosti i raspoloživosti zdravstvenih podataka)***

**Primena na teritoriji:** SAD

**Odnosi se na:** Zdravstveni sektor

**Opis:** Ovaj propis iz 1996. odnosi se na sve američke zdravstvene ustanove. Cilj mu je poboljšanje funkcionisanja zdravstvenog sistema i garantovanje privatnosti zdravstvenog kartona pacijenta. Zahtev za IT je da se poboljša bezbednost i interoperabilnost informacionih sistema, kao i poboljšanje sistema izveštavanja.

## ***Personal Information Protection and Electronic Documents***

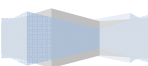
### ***Act (PIPEDA – Canada 2000)***

### ***(Akt o zaštiti ličnih podataka i elektronskih dokumenata)***

**Primena na teritoriji:** Kanade

**Odnosi se na:** Zdravstveni sektor

**Opis:** PIPEDA ima za cilj da izbalansira pravo pojedinca na privatnost sa potrebama organizacija da prikupljaju, koriste ili otkrivaju tuđe lične podatke u legitimne poslovne svrhe. Odnosi se na sve kanadske kompanije i agencije i ograničava upotrebu i otkrivanje ličnih podataka dobijenih u procesu obavljanja posla. Značaj za IT je odgovornost u obezbeđivanju pouzdanih sistema bezbednosti i izveštavanja.



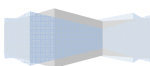
## 4. Ponuda paketa standarda sa *Enthusio™* MSP

Nadležnosti pružaoca IT usluga igraju značajnu ulogu u kontrolisanju usklađenosti sa standardima. Procena usklađenosti sa standardima obično zahteva sprovođenje revizije. Sa aspekta IT, ovi oblici kontrole obično su usmereni na sedam opštih oblasti. Polazeći od ovih oblasti uz primenu *Enthusio™ MSP*, pružalac usluga može da obezbedi rentabilne osnove za sprovođenje takve kontrole.

Ovih sedam komponenti definisao je Američki institut zvaničnih revizora, a poznate su kao **SAS70**. Ispunjavanjem ovih IT stavki, velike organizacije i mala preduzeća mogu da budu sigurni da zadovoljavaju zahteve iz svih gore navedenih zakonskih akata. Drugim rečima, ako se pokaže da poslujete u skladu sa **SAS70**, to je već čvrst pokazatelj da zadovoljavate uslove iz Sarbanes-Oxley, HIPAA i drugih propisa.

Srećom, uz primenu **Enthusio™ MSP**, svih sedam pomenutih zahteva iz IT domena mogu lako i efikasno da se ispune.

IT zahtev	Prednost <b>Enthusio™ MSP</b>
Kontrolisana sredina	Najbolja iskustva u praksi, 24x7 monitoring mreže; dodeljivanje uloga i ovlašćenja; automatsko i ovlašćeno manipulisanje elementima softvera ( <b>patch management</b> )
Fizička zaštita	Monitoring na bazi SNMP-a i WMI-a, dnevnik intervencija ( <b>event logging</b> ), automatsko registrovanje elemenata sistema ( <b>asset</b> )
Postupak u slučaju štete	Planiranje pripravnosti uz prateće izveštaje ( <b>Readiness planning supported by reports</b> ); praćenje najboljih iskustava u praksi; pravljenje rezerve ( <b>backup management</b> ); podrška srodnih službi
Raspoloživost	Trajni nadzor; bezbedno, daljinsko upravljanje u slučaju hitnog uklanjanja kvara; dubinski nadzor kritičnih servera
Bezbednost podataka	Rešenje u skladu sa standardom ISO17799; kontrola pristupa i ovlašćenja sprovođenje revizije; preventivne procene osetljivosti; momentalno registrovanje upada
Bezbednost mreže	Upravljanje Firewall zaštitom; mogućnost automatske nadogradnje elemenata softvera ( <b>automated patching</b> ); integrisanje MBSA
Vidljivost stanja mreže	Sveobuhvatni izveštaji o funkcionisanju i stanju mreže; detaljan inventar elemenata mreže (detailed asset inventories); podrška kod planiranja kapaciteta; komandni pultovi klijenata



## **Pružanje usluga iz kontrolisane sredine**

Ovo se odnosi na to kako upravljate svojim sistemom usluga. Trebalo bi da imate ustanovljene procedure kojih se dosledno pridržavate. Osoblje treba da bude adekvatno obučeno. Moraćete da demonstrirate opredeljenost ka kompetencijama i integritetu. Sa stanovišta poslovanja, zadaci, autoritet i odgovornost moraju da budu jasno raspoređeni.

YUTRO.com i njihovi partneri nude mnoge kurseve i materijale za utvrđivanje najbolje prakse kao što je kreiranje validnih servisnih grupa i procena stanja mreže. **Enthusio™ MSP** vam omogućava da za sve korisnike definišete uloge i ovlašćenja. Doslednost ćete obezbediti kombinacijom jasno definisanih kontrolnih modula (**monitoring Policy Modules**) i politike centralnog rukovođenja grupama (**centrally managed group policies**) u primeni ovih kontrolnih pravila.

## **Obezbeđivanje fizičke zaštite**

Prvi nivo zaštite od upada postiže se kada se obezbedi praćenje i kontrola nad pristupom aktuelnoj opremi. Korišćenjem **Enthusio™ MSP** možete preko SNMP-a da pratite stanje bezbednosti i nadzornih sistema. Mnogi sistemi zasnovani na pristupnim karticama arhiviraju svaki pokušaj pristupa u dnevniku (custom log) koji može i daljinski da se pozove i kontroliše preko **Enthusio™ MSP**.

## **Postupak u slučaju štete**

Neka vaš paket usluga sadrži sledeće: Backup, Restore, Offsite Storage i Backup Performance Monitoring.

Korišćenjem modula **Enthusio™ MSP** možete da ponudite preventivno praćenje *backup* softvera ili putem integrisanja sa srodnim službama možete ove usluge da prebacite na osoblje nadležno za usaglašenost sa standardima. Za klijente kojima je neophodna hitna regeneracija podataka, možete da instalirate i **Enthusio™ MSP** na sajtu za regeneraciju podataka u slučaju štete, kako biste pratili pripravnost rezervnih sistema.

## **Obezbeđivanje raspoloživosti**

Za neke oblike poslovanja, trajna raspoloživost podataka i rada u mreži je od udarnog značaja. To se naročito odnosi na službe u zdravstvu koje su vezane za pacijente. Ovaj paket treba da sadrži usluge kao što su praćenje funkcionisanja sistema, rešavanje problema, pomoć iz prve ruke, ticketing system, automatska dojava i planiranje kontinuiranog posla. Praćenje trajne raspoloživosti predstavlja temelj **Enthusio™ MSP** i uz to možete svojim klijentima da ponudite i dubinski nadzor kritičnih servera i za njih bitnih web sajtova.

## Bezbednost podataka

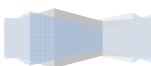
Primenite jasne mehanizme za efikasno upravljanje sopstvenim sistemom i sistemima Vaših klijenata i za kontrolisanje bezbednosti podataka uključujući politiku i procedure za dodelu šifara, praćenje i izveštavanje o neovlašćenom pristupu ili pokušajima pristupa.

**Enthusio™ MSP** rešenje je u saglasnosti sa ISO 17799 standardom koje je prošlo nezavisnu sigurnosnu reviziju za kontrolisanje šifara, za reviziju i za sprečavanje upada u sistem. Na primer, posebni izveštaji poslužiće za procenu sigurnosti MBSA site; Policy moduli nadziraće dnevnik bezbednosnih intervencija (security events log) na kritičnim serverima i *firewall* sistemima zaštite.

## Bezbednost mreže

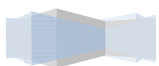
Obezbedite odgovarajuće mehanizme da zaštitite mrežu od neovlašćenog pristupa tako što ćete verifikovati i pratiti *firewall* sisteme zaštite, pratiti pokušaje upada i skenirati osetljivost mreže.

**Enthusio™ MSP** nudi više od 17 Policy modula za najbolji mogući nadzor nad *firewall* sistemima zaštite, a pruža i mogućnost integrisanja MBSA za skeniranje elementarne osetljivosti kod Windows sistema. Obezbedite svojim klijentima mogućnost da prate stanje svoje mreže. Prema propisima, Vaši klijenti su najodgovorniji za rukovođenje svojim poslovanjem, čak i ako su Vama prepustili rukovođenje IT sistemima. Korišćenjem izveštaja preko **Enthusio™ MSP** da biste klijente obavestili o preventivnim popravkama, funkcionisanju i raspoloživosti mreže, tačnim izveštajima iz njihovog okruženja i preciznim izveštajima o inventaru elemenata mreže, Vi im pomažete da funkcionišu u skladu sa ovim standardnim zahtevom. Na primer, Executive Summary izveštaj pokazuje koliko puta su pokrenuti ticket-i i pruža dokaz o vašoj blagovremenoj asistenciji.



## 5. Zaključak

Sa sve većom brigom i uvođenjem sve više propisa u cilju zaštite podataka i imovine, vaši klijenti ne mogu sebi da dozvole ne-standardnu konfiguraciju ili nivo zaštite. **Enthusio™ MSP** Vam omogućava da klijentima ponudite usluge koje su im potrebne kako bi bili zaštićeni i funkcionisali u saglasnosti sa standardima.



---

© 2009 YUTRO.com Sva prava zadržana. Publikacija se ne sme reprodukovati, čuvati na javnim sistemima ili preneti u bilo kojem obliku ili na bilo koji način bez prethodne pismene dozvole YUTRO.com. Iako su preduzete sve mere predostrožnosti i provere, u pripremi ovog dokumenta, YUTRO.com ne preuzima odgovornost za greške ili propuste niti odgovornost za greške nastale korišćenjem informacija iz ovog dokumenta.

Enthusio registrovana marka YUTRO.com.

Adobe i Acrobat registrovane robne marke Adobe Systems Incorporated u SAD, i ostalim zemljama.

Microsoft, Windows, i Windows Server su robne marke ili registrovane robne marke Microsoft Corporation u SAD i ostalim zemljama.

Sve ostale marke, imena proizvoda, imena kompanija, robne marke, i imena servisa su vlasništvo njihovih nosilaca prava.

Verzija 2.01; ažurirano avgust 2009

---

