



Skapat av: Tomas Eiksson    Ägare: Decado AB

Datum: 2009-05-28    Sidan 1 av 15

# Hur bygger man upp en IT-policy?

-Ett dokument från  
Secure-IT.se

Vi innehar F-skattebevis

Momsregistrerings nr SE556650187901

---

**Namn**  
Decado AB

**Adress**  
Box 6111, 800 06 Gävle

**Telefon**  
026-10 02 30

**Fax**  
026-10 19 52

**Org.nr**  
556650-1879

**Säte**  
Gävleborg



Skapat av: Tomas Eiksson    Ägare: Decado AB

Datum: 2009-05-28    Sidan 2 av 15

### Hur bygger man upp en IT-policy?

#### Vad är en IT-policy?

En IT-policy kan enklast förklaras som ett dokument som beskriver hur ett företags filosofi, strategier, policys och rutiner med inriktning på behörigheter, integritet och tillgänglighet kring information och informationssystem ser ut.

#### Behörighet

fastställer vilken typ av information olika medarbetare inom organisationen skall ha tillgång till. Vi vill säkerställa att endast personal med rätt behörighet kan ta del av information som företaget eller organisationen ser som kritisk.

#### Integritet

är en fråga om att säkerställa äktheten i den information som företaget har tillgång till. Information har endast ett värde om vi vet att den är riktig och korrekt.

#### Tillgänglighet

är en fråga om att säkerställa att de IT-system företaget eller organisationen förfogar över finns tillgängliga när så krävs.

#### Vad är fördelarna med en väl uppbyggd IT-policy?

Vi har en viss tendens att luta oss för mycket mot tekniska lösningar när det gäller informationssäkerhets relaterade frågor. Teknik är bra och ett måste för att god informationssäkerhet skall kunna uppnås men vi listar några punkter som talar mot för mycket tilltro till teknik:

#### Falsk trygghet

Det kan vara lätt att tro att bara för att företaget har lagt ut stora belopp på den senaste tekniska utrustningen kan alla inom organisationen luta sig tillbaka i lugn och ro. Så är dock inte fallet, alla system har brister och administreras inte systemen på ett riktigt sätt spelar det ingen roll hur dyra de är.

#### Kompetensbundet

De flesta IT-system kräver en viss grad av kompetens för att administrera. Det gäller från ordbehandlingsprogrammet upp till de mest avancerade delarna av företagets IT-system. Smaka på följande begrepp: Konfiguration av brandvägg, patchhantering av server, uppdatering av regelverk till IDS, skapande av egna regler till IDS, installation av OS, administrera AD mm. Det är förfaranden knutna till få individer med en viss kompetens.

#### Resurskrävande

Teknik är resurskrävande både i form av pengar och mantimmar. En IT-policy är också resurskrävande vid uppbyggnad och implementering. Den skall också ha en ägare (någon med kunskap och kompetens) som ser till att den lever samt efterlevs. Men fördelarna med en väl uppbyggd IT-policy är att alla inom en organisation kan ta del av och efterleva företagets filosofi och strategier gällande specifika situationer. VD för företaget kan ingenting om IDS men han kan ta till sig från IT-policyn att han inte skall klicka på länkar eller bifogade filer i mail från okända avsändare. Han kan också ta till sig att han skall skydda sitt lösenord och han skall också se till att lösenordet byggs upp efter speciella krav. Han kan dock ingenting om AD eller patchhantering.

#### Vad vill vi då ha sagt med detta?

En IT-policy som klargör hur företaget vill att dess personal skall agera i specifika situationer är minst lika viktigt som tekniskt avancerade system. En IT-policy kan alla inom organisationen ta till sig och implementeras den på ett riktigt sätt med god information om varför den anställda skall följa IT-policyn kommer säkerheten kring företagets information höjas avsevärt jämfört med att bara låta tekniska system stå för informationsskyddet.

Vi innehar F-skattebevis

Momsregistrerings nr SE556650187901

Namn	Adress	Telefon	Fax	Org.nr	Säte
Decado AB	Box 6111, 800 06 Gävle	026-10 02 30	026-10 19 52	556650-1879	Gävleborg



Skapat av: Tomas Eiksson    Ägare: Decado AB

Datum: 2009-05-28    Sidan 3 av 15

En annan stor fördel med en IT-policy är att företaget talar om utåt att man tar IT- och informationsrelaterade frågor på allvar. Det ger ökad goodwill till företaget vilket naturligtvis är positivt.

En policy ger oss också andra fördelar. Företaget får ett instrument där man kan ställa insatts mot utkomst. Ett exempel kan vara huruvida en ansvarig inom de IT-relaterade områdena hanterar sina investeringar på bästa sätt. Ställ dennes investeringar och framskridande mot IT-policyn. En väl implementerad IT-policy där samtliga anställda har informerats, accepterat och signerat denna är ett utmärkt verktyg när någon sedan brister i omdöme. Brott mot ett företags IT-policy skall innebära någon form av påföljd, påföljden styrs sedan av brottets allvarlighetsgrad.

En IT-policy talar också om vem som har ansvar för vad vilket är mycket viktigt för att säkerställa att specifika områden administreras på ett riktigt sätt.

En väl uppbyggd och implementerad IT-policy kommer också att fungera som referens för företagets anställda inom IT-relaterade frågor. Policyn talat om vad vi kan göra och vad vi inte kan göra i olika situationer. Detta innebär att en väl fungerade policy gör företagets personal till en del av lösningen istället för en del av problemet. Men utan en fungerande IT-policy kan företaget omöjligt kräva att Kalle, Britta och Sven skall veta hur de skall agera i olika situationer de ställs inför.

*"Det är ju ingen som har sagt nått så jag antar att ungarna kan använda företagets laptop hemma".*

Med en väl utformad IT-policy blir det inga frågetecken. Företaget har som skyldighet att bygga upp och implementera IT-policyn men när det är gjort faller ansvaret ut på varje enskild individ. Det går inte längre att ignorera eller gömma sig bakom "Jag visste inte...".

En IT-policy stärker också den IT-ansvariges position då denna ofta ses som "glädjedödare" då hon eller han försöker att genomdriva åtgärder till gagn för företagets bästa. Om företaget har en IT-policy som är förankrad och godkänd med företagsledningen stärks den IT-ansvariges självförtroende och vetskap om att det han eller hon utför är sanktionerat av företaget. Därmed punkt!

Vi innehar F-skattebevis

Momsregistrerings nr SE556650187901

Namn	Adress	Telefon	Fax	Org.nr	Säte
Decado AB	Box 6111, 800 06 Gävle	026-10 02 30	026-10 19 52	556650-1879	Gävleborg



Skapat av: Tomas Eiksson    Ägare: Decado AB

Datum: 2009-05-28    Sidan 4 av 15



Ett företag med en väl uppbyggd IT-policy som är godkänd, implementerad och accepterad (signerad) i kombination med väl anpassade IT-säkerhetssystem borgar för god informationssäkerhet.

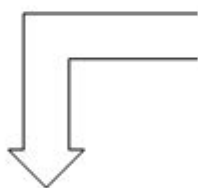


IT-policy

+



IT-säkerhetssystem



= God Informationssäkerhet  
Vi innehar F-skattebevis

Momsregistrerings nr SE55665018/901

Namn	Adress	Telefon	Fax	Org.nr	Säte
Decado AB	Box 6111, 800 06 Gävle	026-10 02 30	026-10 19 52	556650-1879	Gävleborg



Skapat av: Tomas Eiksson    Ägare: Decado AB

Datum: 2009-05-28    Sidan 5 av 15

Hur startar man då arbetet med att bygga upp en IT-policy?

#### Identifiera

Det första som måste göras är att identifiera de risker företaget ställs inför. Vad förfogar företaget över för information och hur exponeras den informationen. All exponering innebär risker och vår målsättning är att kunna exponera vår information men eliminera riskerna. Vi skulle kunna låsa in vår information och kasta bort nyckeln men hur skall vi då kunna bearbeta informationen, vilken glädje har vi av den i det stadiet?

Vårt mål är att reducera riskerna till en nivå som är acceptabel för vår verksamhet oavsett om vi gör det med hjälp av dokument eller fysiska skyddsmekanismer.

Vi måste identifiera de områden som är svagast och börja med dessa. En policy kan alltid utökas vilket innebär att det inte finns någon anledning att inkludera alla bitar på en gång. Analysera vad som är företagets mest kritiska information samt hur den informationen hanteras idag. Vi vill kunna exponera den informationen men vi vill reducera riskerna vid exponering.

Vi innehar F-skattebevis

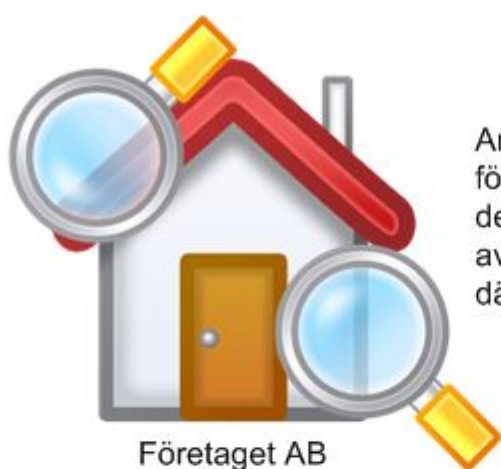
Momsregistrerings nr SE556650187901

Namn	Adress	Telefon	Fax	Org.nr	Säte
Decado AB	Box 6111, 800 06 Gävle	026-10 02 30	026-10 19 52	556650-1879	Gävleborg



Skapat av: Tomas Eiksson    Ägare: Decado AB

Datum: 2009-05-28    Sidan 6 av 15



Analysera vilken information företaget förfogar över. Identifiera de svaga punkterna vid exponering av denna information för att därefter kunna reducera riskerna.

Företaget AB förfogar över viss typ av information som man önskar exponera.



Information



Information

Man kan lätt invaggas i tron att det går att "titta på" en befintlig IT-policy och därefter implementera den i organisationen. Naturligtvis kan vi få nyttig information och en plattform att börja bygga på genom att titta på hur en befintlig policy är uppbyggd. Men passar den din organisation? Alla företag är unika i fråga om företagskultur samt tillvägagångssätt i olika situationer samt också vilken typ av information vi hanterar vilket gör att en IT-policy också i slutänden kommer att vara unik för företaget. På Secure-IT.se och Secure IT Premium lämnar vi förslag till IT-policys som ni får använda precis som ni önskar men ställ varje punkt i dessa policyförslag mot den organisation du tillhör innan du implementerar någon av dessa policys.

Vi innehar F-skattebevis

Momsregistrerings nr SE556650187901

**Namn**

**Adress**

**Telefon**

**Fax**

**Org.nr**

**Säte**

Decado AB

Box 6111, 800 06 Gävle

026-10 02 30

026-10 19 52

556650-1879

Gävleborg



Skapat av: Tomas Eiksson    Ägare: Decado AB

Datum: 2009-05-28    Sidan 7 av 15

### Förankra

Alla typer av policys är verkningslösa om de inte förankras i företagets ledning. Företagsledningen måste backa upp alla delar i policyn och ställa sig bakom dessa när policyn utsätts för hetluft från organisationen. Naturligtvis är det lika viktigt att företagsledningen står bakom den som utses att ansvara för policyns efterlevnad, att backa från dessa punkter är att skjuta policyn i sank ögonblickligen. Det blir naturligtvis svårare att komma tillbaka vid ett senare tillfälle med nya förslag till policys om detta inträffar vilket gör att detta arbete måste genomdrivas på bästa tänkbara sätt.

Företagsledningen måste med andra ord förstå vikten av att skydda den information företaget förfogar över. Riskerna vid exponering måste påvisas och när detta gäller exponering via IT-relaterade system kan det bli en längre vandring att beskriva detta men det måste göras. Alla inom företagsledningen måste förstå varför en IT-policy behövs och när alla förstår alla delar måste ledningen ställa sig bakom framtagandeprocessen samt den färdiga IT-policyn till hundra procent.

Vi innehar F-skattebevis

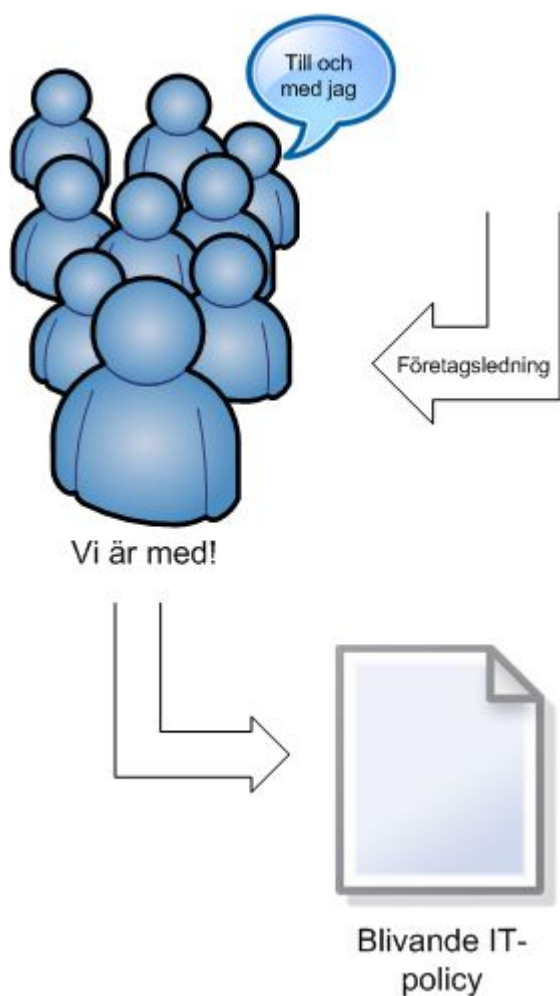
Momsregistrerings nr SE556650187901

Namn	Adress	Telefon	Fax	Org.nr	Säte
Decado AB	Box 6111, 800 06 Gävle	026-10 02 30	026-10 19 52	556650-1879	Gävleborg



Skapat av: Tomas Eiksson    Ägare: Decado AB

Datum: 2009-05-28    Sidan 8 av 15



### Ägande

Oavsett hur företagets organisation ser ut skall en ansvarig (ägare) för IT-policy utses. Ofta brukar man utse den IT-ansvarige att ansvar för IT-relaterade dokument men om företaget inte har någon med den befattningen skall ändå en ägare av IT-policy utses. Vi betitlar hädanefter denna befattning som 'Ägaren'. Ägarens uppgift är att se till att IT-policyn skapas, distribueras och implementeras. Ägaren skall jobba i samförstånd med företagsledningen från start och dessa två parter skall vara överens om gången för att ta fram en fungerande IT-policy. Det är också ägarens uppgift att med hjälp av företagsledningen samt de olika kompetensområdena (avdelningarna) inom företaget inventera den information företaget förfogar över samt hur den exponeras för att finna de svaga punkterna. Ägaren kommer också att fungera som mellanhand mellan företagsledningen och övriga anställda vilket gör att ägaren oavsett titel bör upplyftas inom organisationen. Ägarens roll bör definieras och dennes ansvar inom organisationen skall fastställas.

Vi innehar F-skattebevis

Momsregistrerings nr SE556650187901

**Namn**

**Adress**

**Telefon**

**Fax**

**Org.nr**

**Säte**

Decado AB

Box 6111, 800 06 Gävle

026-10 02 30

026-10 19 52

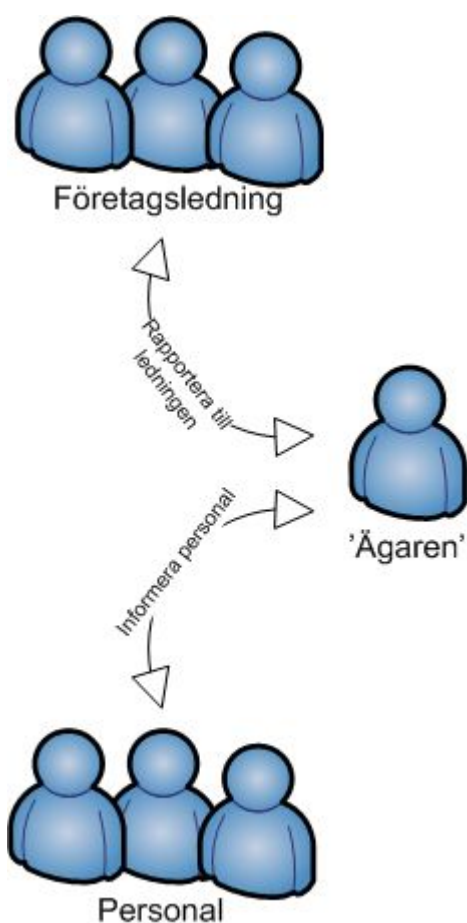
556650-1879

Gävleborg



Skapat av: Tomas Eiksson    Ägare: Decado AB

Datum: 2009-05-28    Sidan 9 av 15



#### Ekonomi

Att ta fram en IT-policy kostar initialt pengar och en väl fungerande och levande IT-policy kostar också pengar under hela dess livscykel. Att säkerställa en IT-policys fortlevnad kostar också tid och humant kapital. Dock skall vi hela tiden komma ihåg att en väl uppbyggd och implementerad IT-policy kommer att generera betydligt mer än den kostar. Detta eftersom vi enkelt kan ställa de ekonomiska aspekterna med att ta fram en IT-policy som uppfyller alla kriterier för en väl fungerande policy mot en avsaknad av IT-policy där anställda ges möjlighet till att hantera information och system på ett felaktigt (kanske till och med kriminellt) sätt. Vi kan naturligtvis också baka in goodwill frågan i detta för att ytterligare fastställa fördelarna med en IT-policy.

Vi innehar F-skattebevis

Momsregistrerings nr SE556650187901

**Namn**

**Adress**

**Telefon**

**Fax**

**Org.nr**

**Säte**

Decado AB

Box 6111, 800 06 Gävle

026-10 02 30

026-10 19 52

556650-1879

Gävleborg



Skapat av: Tomas Eiksson Ägare: Decado AB

Datum: 2009-05-28 Sidan 10 av 15

### Skapa förståelse

Den svagaste länken i en företagsorganisation är vi, människorna bakom tangentborden. Människan är av naturen lat, smart och anpassningsbar för nya situationer. Detta innebär att om något dyker upp som vi upplever som ett "hinder" för våra vardagliga sysslor kommer vi försöka att ta oss runt detta hinder på enklast och snabbast möjliga sätt. Ett typiskt exempel på detta är administration av lösenord.

Om vårt företags IT-policy säger att alla anställda skall byta sitt lösenord 12 ggr per år och lösenordet skall bestå av minst 6 tecken kommer med all säkerhet följande scenario uppstå:

januari: Pinglan1  
februari: Pinglan2  
mars: Pinglan3  
osv...

Vi vill göra det enkelt för oss och genom att lägga upp följande "strategi" bryter vi inte heller mot de krav som företags IT-policy ställer. Hur kommer man då runt detta som 'Ägare' till en IT-policy?

Vi ger några förslag:

### Utbilda medarbetarna

Utbilda medarbetarna i IT-säkerhetsrelaterade frågor. Få dem att förstå konsekvensen av svaga och upprepade lösenord. Få dem att förstå riskerna med att sprida känslig information över hela företaget och framförallt utanför företaget. Få dem att förstå riskerna med att skicka känslig information okrypterat via e-post. Få dem att förstå riskerna med att klicka på länkar i mail från okända avsändare. Lägg upp en utbildningsplan där IT-policyn ligger som grund.

### Fokusera på mellancheferna

Mellanchefer är 'Ägarens' bästa vänner när det gäller att förmedla ett budskap ut i organisationen. Men för att mellancheferna skall kunna göra detta på bästa sätt måste de förstå innebörden av IT-policyn och även förstå de olika hotbilder företags information ställs inför varje dag. En duktig mellanchefer kan få vilken avdelning som helst på fötter och köper hon eller han det koncept du som 'Ägare' förmedlar har du även vunnit hela den underliggande avdelningen.

### Var ärlig

Var ärlig mot medarbetarna, informera om de risker företags informationsflöde ställs inför varje dag. Genomför en säkerhetsanalys och redovisa resultatet i kombination med information om hur företaget kan förbättra de svaga punkterna. Får de anställda ökad förståelse för säkerhetsrelaterade frågor kommer det fortsatta arbetet att gå mycket enklare.

### Morot och piska

När företaget har implementerat sin IT-policy går det att jobba med mätbara resultat av denna implementering. Medarbetare som efterlever IT-policyn och kanske gör det till sådan grad att de kommer med förslag om förbättringar skall belönas för sin lojalitet. På andra sidan skall det finnas klara konsekvenser med att bryta mot en implementerad IT-policy. Vi har nämnt det förut men det är värt att göra det igen, för att en IT-policy skall ha något värde måste ett av de uppfyllda kraven vara att den är accepterad och signerad av varje anställd inom företaget. Bara då kan man gå tillbaks och prata konsekvenser med en medarbetare.

Vi innehar F-skattebevis

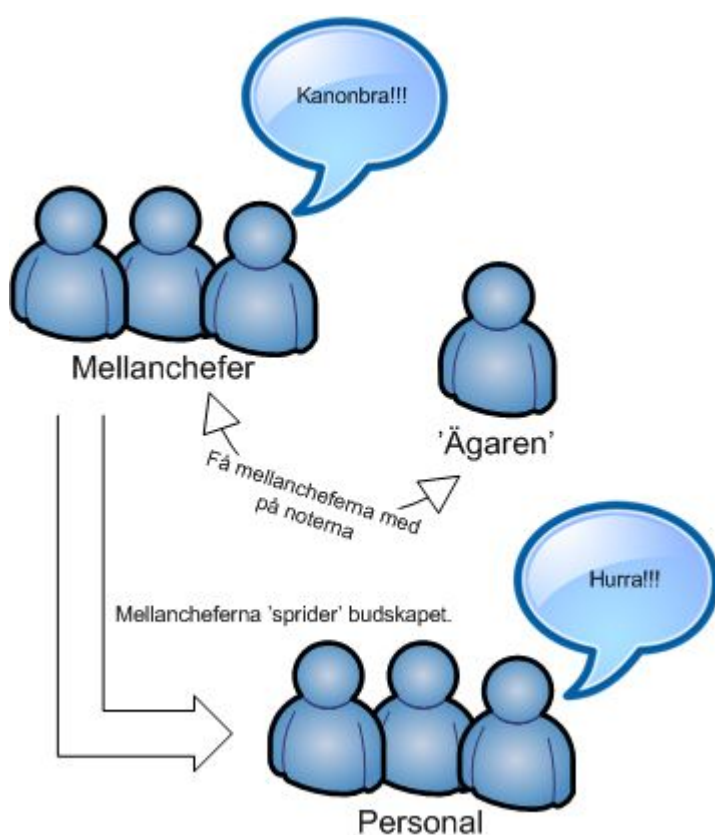
Momsregistrerings nr SE556650187901

Namn	Adress	Telefon	Fax	Org.nr	Säte
Decado AB	Box 6111, 800 06 Gävle	026-10 02 30	026-10 19 52	556650-1879	Gävleborg



Skapat av: Tomas Eiksson    Ägare: Decado AB

Datum: 2009-05-28    Sidan 11 av 15



### Klassificera informationen

All känslig information inom ett företag måste klassificeras, att bara sätta en etikett som säger "Endast behörig personal har tillträde till känslig information" är fullständigt verkningslöst om det inte framgår vilka som omfattas av begreppet behörig personal samt vad som är känslig information. Klassificeringen skall sedan styra behörigheten till olika typer av information. Skapa ett klassificeringssystem inom företaget och stoppa medarbetarna i olika containrar där varje container har tilldelats behörighet till en viss typ av klassificerat material. Klassificeringen kan bygga på Oklassificerat material, Begränsad tillgång, Känsligt material och Hemligt material.

Vi innehar F-skattebevis

Momsregistrerings nr SE556650187901

**Namn**

**Adress**

**Telefon**

**Fax**

**Org.nr**

**Säte**

Decado AB

Box 6111, 800 06 Gävle

026-10 02 30

026-10 19 52

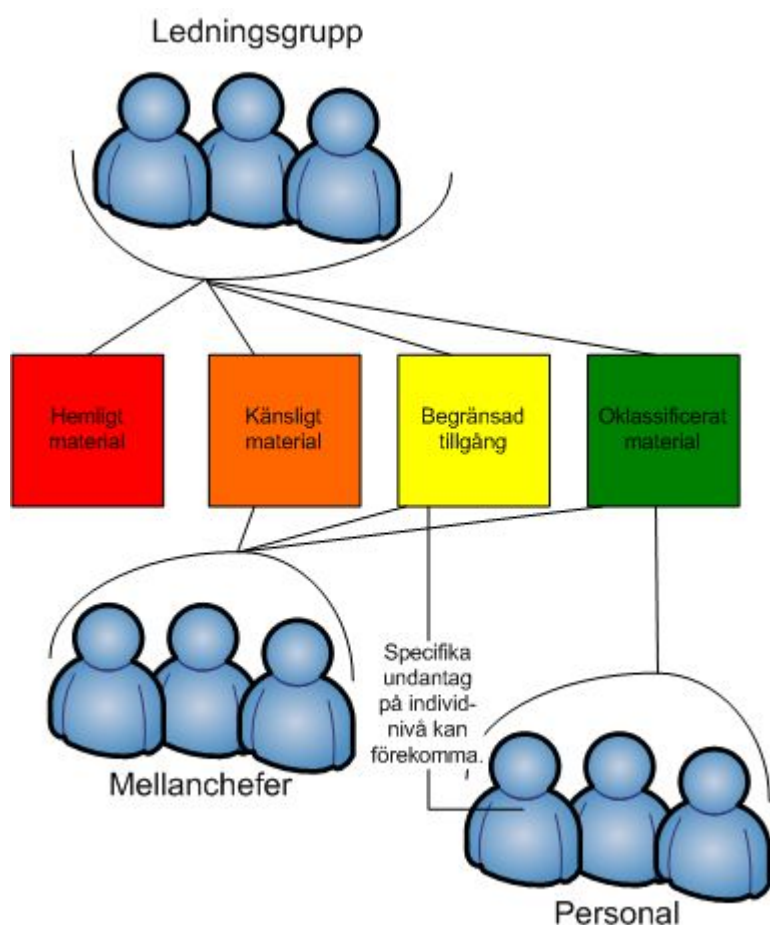
556650-1879

Gävleborg



Skapat av: Tomas Eiksson    Ägare: Decado AB

Datum: 2009-05-28    Sidan 12 av 15



### Omfattning

Det bör fastläggas vilka IT-policyer omfattar. Det kan ses som en självklarhet att personalen som är fast anställd av företaget omfattas av IT-policyen. Men hur skall företaget förhålla sig till inhyrd personal, underentreprenörer, semestervikarier, sommarvikarier mfl. Ett klart svar på detta är att all personal som utför arbete åt företaget där arbetet är av sådan art att företagets information kommer att hanteras av den anställde skall omfattas av företagets IT-policy. Detta innebär således att samtliga av dessa kategorier skall erhålla samma implementeringsförfarande som fast anställd personal.

Vi innehar F-skattebevis

Momsregistrerings nr SE556650187901

**Namn**  
Decado AB

**Adress**  
Box 6111, 800 06 Gävle

**Telefon**  
026-10 02 30

**Fax**  
026-10 19 52

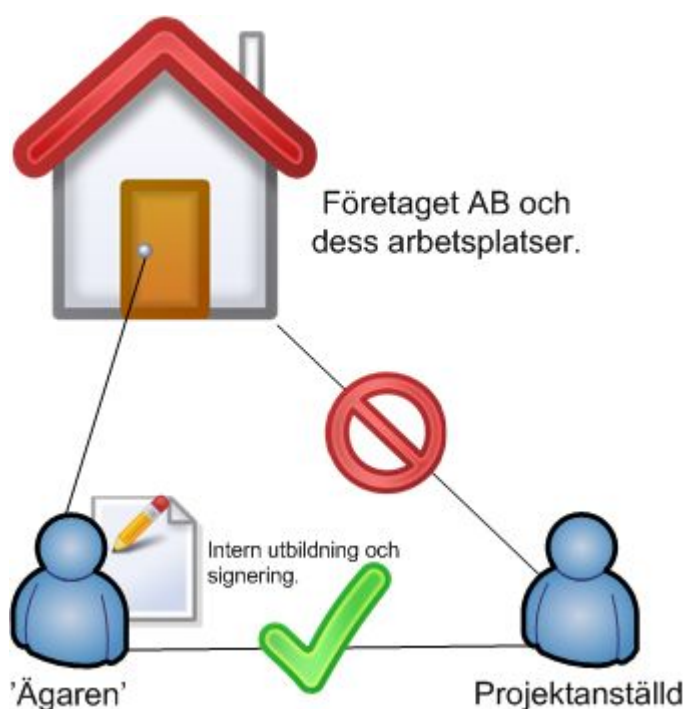
**Org.nr**  
556650-1879

**Säte**  
Gävleborg



Skapat av: Tomas Eiksson    Ägare: Decado AB

Datum: 2009-05-28    Sidan 13 av 15



#### Håll policyn kort och koncis

En IT-policy skall skapas utifrån de förutsättningar som gäller för det specifika företaget. Vi har talat om att identifiera de risker företaget ställs inför. Vad förfogar företaget över för information och hur exponeras den informationen. När vi har fått svaren på dessa frågor kan vi börja bygga upp vår policy. En rekommendation är att hålla policyn så kort och koncis som möjligt. En IT-policy måste vara strukturerad samt förpackad på sådant sätt att information är lätt att finna och ta till sig. Om vi talar om en större organisation kan policyn delas upp i specifika delar (eller områden). Det är också bra om IT-policyn är enkel att administrera och underhålla, vi skall komma ihåg att det är ett levande dokument som kommer att uppdateras beroende på vilka faser företaget och dess informationssystem genomgår.

Vi innehar F-skattebevis

Momsregistrerings nr SE556650187901

**Namn**

**Adress**

**Telefon**

**Fax**

**Org.nr**

**Säte**

Decado AB

Box 6111, 800 06 Gävle

026-10 02 30

026-10 19 52

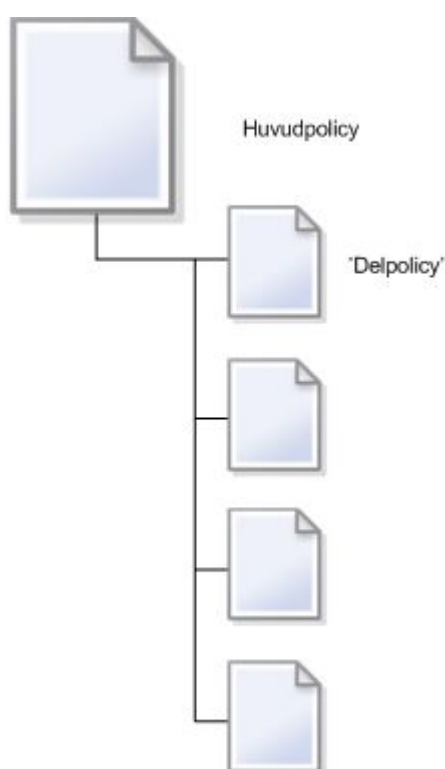
556650-1879

Gävleborg



Skapat av: Tomas Eiksson    Ägare: Decado AB

Datum: 2009-05-28    Sidan 14 av 15



### Glöm inte bort incidenter och incidentrapportering

Vissa specifika delar i en IT-policy kan behöva en beskrivning som redogör vad användarna skall göra vid händelse av en incident. Det kan också rekommenderas att incidentrapportering tas upp i IT-policyn. Hur skall incidenter rapporteras och till vem.

### Extern dokumentation

Vissa delar i en IT-policy kan komma att hänvisa till extern dokumentation. Om så är fallet skall den dokumentationen redovisas korrekt i policyn samt förvaras och hanteras på ett fastställt sätt.

### Konsekvenser

Vad händer om någon inom organisationen bryter mot IT-policyn? Det skall framgå klart och tydligt i policyn vad medarbetarna kan förvänta sig för konsekvenser om de bryter mot någon del av denna. Konsekvenserna bör ställas mot den regelöverträdelse som har inträffat vilket innebär att den lägre skalan av konsekvens kan vara en muntlig varning, därefter skriftlig varning och slutligen avstängning från företagets IT-system. Allvarliga överträdelser kan generera ett avskedande från företaget och vid överträdelser som bryter mot rikets lagar kan det bli fråga om en polisanmälan, allt är beroende på överträdelsens allvarlighetsgrad.

Vi innehar F-skattebevis

Momsregistrerings nr SE556650187901

Namn	Adress	Telefon	Fax	Org.nr	Säte
Decado AB	Box 6111, 800 06 Gävle	026-10 02 30	026-10 19 52	556650-1879	Gävleborg



Skapat av: Tomas Eiksson    Ägare: Decado AB

Datum: 2009-05-28    Sidan 15 av 15

### Egen kontroll

'Ägaren' bör med jämna mellanrum utföra interna kontroller som fastställer hur IT-policyn efterlevs. Detta är ett effektivt instrument för att hålla samtliga inblandade parter inom ett organisationen medvetna om IT-policyns betydelse för företaget.

'Ägaren' kan även rikta frågor några till sig själv:

- Är IT-policyn godkänd av företagsledningen?
- Är det fastställt vilka system och personer IT-policyn gäller?
- Är alla kritiska delar i företagets informationssystem inkluderade i IT-policyn?
- Fastställer IT-policyn på ett klart sätt vilket ansvar de olika personerna inom organisationen har?
- Är IT-policyn formbar, kan den enkelt uppdateras för att täcka in nya tekniker och hotbilder?
- Är IT-policyn upplagd på ett konkret och riktigt sätt?
- Är IT-policyn implementerad och införstådd hos samtliga medarbetare?
- Är IT-policyn signerad av samtliga medarbetare?
- Finns det en plan för intern utbildning av nya anställda samt inhyrd personal och extra personal?
- Levererar IT-policyn önskad effekt?

Vi hoppas att du har haft glädje av detta dokument och vi önskar lycka till med ditt fortsatta policyarbete.

Namn	Adress	Telefon	Fax	Org.nr	Säte
Decado AB	Box 6111, 800 06 Gävle	026-10 02 30	026-10 19 52	556650-1879	Gävleborg

Vi innehar F-skattebevis

Momsregistrerings nr SE556650187901