Informationssäkerhetspolicy för Mätarkontroll i Stockholm AB

Syftet med denna policy är att Mätarkontroll i Stockholm AB inom branschen ska ses som ett föredöme och en långsiktigt trygg professionell samarbetspartner. Genom att skydda våra affärshemligheter och kunders intressen får företaget ett gott anseende i branschen och en hållbar långsiktig utveckling.

Att ha kontroll över all information i ett företag är både komplext och krävande. I kravbilden för Mätarkontroll ingår de krav på dokumentstyrning och sekretess som följer av våra ackrediteringar. I övrigt måste varje seriöst företag veta hur information ska hanteras och klara av detta i praktiken. Här sätter vi själva ribban, både utifrån yttre förväntningar i ett snabbt växande informationssamhälle och utifrån ledningens ambitioner och planer, som en integrerad del av koncernens strategi och affärsplanering.

Komplexiteten blir stor i dagens informationsflöden när ökad effektivitet driver upp takten och informationsmängden. Detta sker parallellt med större krav på sammankoppling av olika sorters information. Samtidigt intensifieras hotbilden när datorer och nätverk blir vårt främsta hjälpmedel för att klara detta. Olagliga intrång och dataförlust kan få katastrofala följder – att sådant inte inträffar måste säkerställas.

Strukturering av information – informationsmatris

För att hantera komplexiteten har Mätarkontroll definerat en ”informationsmatris” som ger tydlig struktur åt olika typer av information och motsvarande krav som måste ställas för att vi ska upprätthålla de krav man kan förvänta sig av ett modernt företag i infomationsåldern. För att hantera hotbilderna definieras också en delpolicy för datasystemdriften i företaget (se längst ned i detta dokument).

Vi delar först in informationen i fyra slag av information:

1. Information om företagets samlade kompetensresurs (personal och organisationskompetens). Mycket information här utgör själva kompetensresursen.
2. Information relaterad till kunder och deras provningsobjekt/utrustning. Även objekten i sig själva är att betrakta som informationsbärare.
3. Information relaterad till företagets affärer – såväl affärshemligheter som marknadsförings- och försäljningsinformation.
4. Information om företagets hårda resurser – provningsutrustning, hjälpmedel och lokaler.

Som andra steg delar vi in informationens hantering och egenskaper i fyra nyckelfaktorer som är allmänt etablerade nyckelfaktorer för informationssäkerhet:

1. Riktighet – all information som Mätarkontroll producerar ska vara riktig. Övrig information ska granskas så långt det är rimligt för att riktighetskravet ska vara uppfyllt.

2. Tillgänglighet – *när* informationen behövs, ska den som är *behörig* lätt hitta den, *där* den behövs. Denna åtkomst måste garanteras – informationsförlust kan ej accepteras. I denna punkt ingår hänsyn till att IT-system i vilka information lagras antingen kan återställa utrangerade programvaror som krävs för att information ska kunna läsas eller att informationen i sig uppdateras formatmässigt för läsning i nyare system. Detta gäller under specifika tidsintervall definierade för olika dokumenttyper.
3. Sekretess – endast de som har legitim anledning att erhålla en viss sorts information ska få tillgång till den. För övriga ska informationen vara skyddad. Behörighet för individer bestäms av ledningen som en del av det löpande organiserandet av arbetet och ingår som övervägande i planering och genomförande av kompetensutveckling. Knutet till sekretessbegreppet är konfidentialitet – en kund som samtalar med en medarbetare ska kunna lita på att informationen inte förs vidare.
4. Spårbarhet – både när det gäller affärer/avtal och när det gäller den ackrediterade verksamheten ställs krav på spårbarhet. Det ska i efterhand gå att se hur informationen kommit till, vem som ansvarat för detta och vilka avgränsningar som gäller/vilken situation den relaterar till. Här ingår tydliga referenser till andra imformationskällor. När ett dokument har ändrats ska det gå att spåra dessa ändringar tillbaka i varje steg.

För varje slag av information (enligt första listan ovan) ska de fyra nyckelfaktorerna (enligt andra listan) uppfyllas på olika sätt beroende på vilken funktion informationen har. Vi får följande matris (som har utvidgats något – se kommentarer):

		Riktighet	**Tillgänglighet**	**Sekretess**	**Spårbarhet**
Kompetens-resurser	**Roller**	Ledningen	Medelhög	Låg	Medel
	Personer	Chef/medarb.	Medelhög	Restrikt.	Hög
Kunder	**Affärer/avtal**	Ansv./kund	Hög	Restrikt.	Mkt hög
	Provningsresultat	Ansvarig	Hög	Hög	Mkt hög
Affärer/ marknad	**Beskrivande**	Ledningen	Medehög	Låg	Medel
	Strategisk	Ledningen	Medelhög	Hög	Hög
Utrustning etc.	**Tillverkares**	Tillv./ansv.	Hög	Medelhög	Hög
	Rutiner/data	Ansvarig	Hög	Hög	Mkt hög

Kommentarer:

Under *riktighet* anges ansvar för informationen. Matrisen visar vem/vilka som är ansvariga för informationens riktighet. Detta gäller för det tillfälle då information sammanställs till en enhet för vidare hantering, t.ex. att ett dokument utfärdas eller en datafil genereras ur ett mätdata-system. Riktighet kan inte alltid garanteras eller fullt ut kontrolleras av den ansvarige, men denna ska så långt det är rimligt säkerställa riktigheten. Det är också viktigt att källinformation framgår, så att det senare går att göra riktighetsbefömningar om någon oklarhet uppstår.

Tillgänglighet kopplas till behörighet så att tillgängligheten ska garanteras med viss grad av enkelhet för den som är behörig. Behörigheter tilldelas roller/personer av ledningen och finns detaljerat angivet i rollbeskrivningarna. Matrisen anger den grad av tillgänglighet för envar behörig som eftersträvas. Hög tillgänglighet innebär att informationen i princip ska kunna nås direkt via framtagning ur pärm/mapp eller efter behörig inloggning. En låg tillgänglighet

innebär att det kan ta tid och kräva vissa operationer för åtkomst – t.ex hämtning ur låst arkiv i annan lokal eller återställande av säkerhetskopia på långsamt datamedium.

Sekretess är kopplad till behörighet, fast ”omvänt” mot tillgänglighet – åtkomst ska hindras för alla som saknar behörighet. Denna framgår enligt föregående punkt. Matrisen ovan anger sekretessgrad. Sekretess anger därigenom själva informationens grad av skydd mot åtkomst. I tabellen anges denna åtkomst i förhållande till anställd personal eller jämställda. Sekretessen gäller informationen som sådan, oavsett medium. Det innebär tystnadsplikt när det gäller muntlig sekretessbelagd information.

Spårbarhet är beroende av klassificering, ansvar och märkning. Genom att veta vilken kategori informationen tillhör och hur den är märkt upprätthåller man en dokumentstyrning som garanterar spårbarhet. Matrisen anger grad av krav på spårbarhet. Företagets dokument-styrningssystem är avsett att garantera spårbarhet.

Hanteringskrav på anställda för de fyra nyckelfaktorerna

Ovan nämnda nyckelfaktorer för informationssäkerhet ställer olika krav på dem som hanterar informationen – i det följande beskrivs vad som förväntas av den anställde på principiell nivå:

1. Riktighet – den som, oavsett behörighetsnivå, producerar information/dokument av något slag har ansvar för att den är riktig. Om olika typer av information ingår i ett egetproducerat dokument, så att vissa delar av dokumentationen är omöjlig att kontrollera – yttre källa – ska referenser anges. Sådan information ska dock granskas så långt det är rimligt för att uppfylla riktighetskravet.
   Dokument som produceras ska vara kopplade till behörighet och ansvar, så att innehållet behandlar sådana faktorer som ingår i behörigheten. Om någon annan än ansvarig/behörig producerar information/underlag ska detta kontrolleras och godkännas av ansvarig, som också står som dokumentägare.
2. Tillgänglighet är strikt kopplat till behörighet – en viss typ av information ska vara tillgänglig för behöriga, men inte tillgänglig för övriga.
   Tillgänglighet kan delas in i två huvuddelar – återvinning och åtkomst:

   I *återvinning* ingår att hitta informationen och se till att den är läsbar. Här ingår register-/söksystem och återställande av läsbarhet för äldre datafilstyper.

   Åtkomst rör de konkreta arrangemangen för att åstadkomma och säkerställa läsning/hantering av informationen för den som är behörig.

   Behörighet för olika *roller*, liksom för personer som inte direkt arbetar med kontroll- och kalibreringsverksamheten, definieras av ledningen efter rådande organisation. Behörighet för *personer (rollinnehavare) i den operativa ackrediterade verksamheten* definieras av laboratoriets tekniska ledning, f.n. Mätplatsansvarig.

   Ledningen ska tillse att såväl IT-system som den fysiska miljön fungerar för att upprätthålla tillgänglighet.

3. Sekretess – endast de som genom sina arbetsuppgifter har legitim anledning att erhålla information ska få tillgång till den. För övriga ska den vara skyddad. För individen ingår att vara helt införstådd med sina behörigheter och att inte försöka få tillgång till information som faller utanför dessa. Vidare ingår att veta vad en viss sekretessnivå konkret innebär: hög sekretess innebär att endast informationsägare ska ha tillgång (kundinformation får endast hanteras av anställda som har detta till sin uppgift respektive av vissa personer (beställare) hos kundföretaget; medelhög sekretess innebär att även sådana som är organisatoriskt berörda har tillgång; restriktion innebär att vissa avgöranden av informationsägare ska göras före åtkomst; låg sekretess ger i princip alla anställda (motsv.) tillgång. Det senare gäller t.ex. kvalitetshandböckerna, vars innehåll bör åtminstone vara översiktligt känt av alla – ledningen vill uppmuntra alla anställdas åtkomst. Obehöriga i detta fall är alla som inte är engagerade i företagets verksamhet.
   Skydd ska vara effektivt mot olika försök till obehörig åtkomst på rimliga nivåer. Fysiskt skydd kan åstadkommas genom olika grader av fysisk avgränsning och inlåsning. Logiskt skydd (i IT-system) kan åstadkommas genom tydliga strukturer för behörighets- och sekretessnivåer och deras matchning.
4. Spårbarhet – både när det gäller affärer/avtal och när det gäller den ackrediterade verksamheten ställs krav på spårbarhet. Det ska i efterhand gå att se hur informationen kommit till, vem som ansvarat för detta och vilka avgränsningar som gäller/vilken situation den relaterar till. En åtgärd för spårbarhet är identifiering av ett dokument/en datafil på ett säkert sätt. Exakt hur detta ska göras ska definieras under avsntt för dokumentstyrning i våra kvalitetshandböcker.
   Spårbarhetskravet ställer viktiga krav på dem som åstadkommer, sätter samman eller förändrar information. Var och en som framställer ett dokument, oavsett nivå eller typ av dokument, som är del av eller viktigt för företagets kvalitetsledningssystem ska känna till denna policy och tillsammans med kollegor och ledning verka för att skapa rutiner och mallar etc. som underlättar efterföljandet.

IT-strategi

Mätarkontrolls IT-struktur ska ha tyngdpunkten på driftsäkerhet, funktion och återställning av systemet. Nätverket ska vara tillgängligt dygnet runt både från den fysiska lokalen samt på annan ort via VPN-förbindelse. Filservern ska vara strukturerad utefter avdelningar och verksamhetsområden samt vara behörighetsskyddad.

Varaktigheten på elektroniskt sparade dokument säkerhetsställs genom ”backup” som förvaras på annan ort. Denna tjänst köps in av en extern leverantör och ska ske med automatik via Internet 1 ggr/dygn. Vid totalt haveri eller stöld ska vi kunna bedriva verksamheten som vanligt efter 48 timmar.

Elektroniska dokument
Varaktigheten på elektroniskt sparade dokument säkerhetsställs genom ”backup” som förvaras på annan ort.