IT-policy

Ver 1.3 (under ombearbetning)

Upprättad 2016-01-22

Anders Gerby

IT-policy - utkast

Innehåll

1 Inledning

Med utgångspunkt i Moderaternas politiska verksamhet och de affärsmässiga krav som partiets ledning, förtroendevalda och medlemmar ställer på organisationen, gäller följande regler för anställdas IT-användning. I tillägg till reglerna har vi angett rekommendationer som syftar till att minimera olika typer av risker t.ex. förlust av data. Se terminologi nedan.

Eftersom IT är ett begrepp som är i ständig förändring skall detta dokument inte ses som något slutgiltigt eller statiskt. Det åligger den eller de som ansvarar för detta dokument att informera ledningen och Riksorganisationens anställda om förändringar av detta dokuments innehåll.

1.1 Terminologi

Några begrepp som används i detta dokument:

Regler; med regler avses de avsnitt av policyn som ska följas.

Rekommendationer; med rekommendationer avses de avsnitt som syftar till att ge stöd och hjälp för att minimera risker av olika slag.

IT; Med IT avses i detta dokument såväl de tillämpningssystem, tjänster m.m. som leder till direkt nytta för verksamheten samt den underliggande teknik som möjliggör systemens användning, t ex utrustning, kommunikationsnät, bärartjänster för trådlös datakommunikation, telefoni och operativsystemliknande funktioner.

Mobila plattformar; Mobiltelefoner, läsplattor samt bärbara datorer.

Mjukvara; program som används i en dator för att utföra en uppgift, såsom ordbehandling, e-post, m.m.

Hårdvara; utrustning såsom mobiltelefon, skrivare, tangentbord, dator och bildskärm.

HAG; en säkerhetslösning som medger access till webbaserade applikationer via installerat certifikat och engångslösenord (OTP).

Lagringsmedia; material eller mekanism som tillhandahåller funktionalitet för att lagra digitalt data permanent. Exempel på lagringsmedia är USB-minne, CD-ROM, DVD, hårddisk, digitalminne.

IT-verktyg; IT-baserade arbetsredskap såsom e-post, internet, datorer, telefoner, skrivare samt tillhörande mjukvara, hårdvara och lagringsmedia.

RO; förkortning av Riksorganisationen.

1.2 Syfte

Syftet med IT-policyn är att beskriva de regler och rutiner som gäller för medarbetare och förtroendevalda som använder partiets IT-utrustning. Den redogör även för åtgärder som syftar till att förebygga störningar och otillbörlig informationsspridning.

Moderaternas IT-policy syftar också till att skydda anställdas integritet eftersom var och en då kan agera utifrån de förutsättningar som gäller och att skydda partiets affärskritiska system och varumärket Moderaterna.

1.3 Omfattning

Denna IT-policy gäller digital insamling, bearbetning, lagring, överföring och presentation av data inklusive mobila plattformar

Denna IT-policy fastställs av partiets ledningsgrupp och kompletterar lagar, förordningar, partiets etiska regler samt övriga beslut och styrdokument.

Denna IT-policy gäller alla anställda i partiet, tillfälligt inhyrd arbetskraft samt personer som i sin tjänsteutövning agerar på uppdrag av arbetsgivaren, inkluderande medarbetare eller förtroendevald som använder arbetsgivarens datorutrustning eller telefoniutrustning med eller utan nätverksaccess.

För anställda gäller reglerna i denna policy i tjänsten, men även vid privat användning av arbetsgivarens datorer och mobila terminaler.

1.4 Ansvar

Varje chef ansvarar för att denna policy sprids och efterlevs av anställda, det är också varje chefs ansvar att följa upp att policyn följs.

I samband med implementeringen av denna policy samt vid varje nyanställning inom Moderaterna skall den anställde erhålla ett exemplar där vederbörande skriftligen intygar att denne har tagit del av Moderaternas IT-policy. Genom att ta del av policyn är anställd införstådd med att också följa Moderaternas IT-policy vid varje gällande tidpunkt.

2 Fysisk säkerhet

Den primära fysiska säkerheten eller ”skalskyddet” upprättas genom traditionella säkerhetsanordningar såsom dörrlås, portkoder, larmsystem, passerkort, brandskydd, m.m. Om sådan utrustning eller skydd åsidosätts genom att en anställd släpper in gäster i arbetsgivarens lokaler, så ansvarar den anställde för dessa gäster till dess att de lämnar arbetsgivarens lokaler. Om fel upptäcks av anställd i sådan utrustning eller skydd, är det den anställdes skyldighet att meddela ansvarig funktion i partiet.

3 Information och sekretess

Information som kan anses vara intern partispecifik får inte spridas utanför partiet. Exempel på sådan information är kommunikation med medlemmar, icke-publika uppgifter om medlemmar, åtkomstinformation såsom användarnamn och lösenord och icke-publika uppgifter om arbetsgivaren och dess anställda. Att sprida informationen inkluderar, men är inte begränsat till, förmedling av information via nätverk som Internet och kopiering till lagringsmedia eller annan dator som sedan flyttas från arbetsgivaren.

Arbetsgivaren skall ej missbruka uppgifter eller annan information om anställda även efter anställningens upphörande. Arbetsgivaren skall i den mån det är möjligt inte använda en anställds personnummer för att på ett inom partiet unikt sätt identifiera den anställde. Vad gäller generell hantering av personuppgifter hänvisar denna IT-policy till vid varje tillfälle gällande personuppgiftslag (PUL).

3.1 Åtgärder vid förlust eller skada

Vid förlust av arbetsstation, lagringsmedia, mobiltelefon eller annan utrustning innehållande partispecifik information, skall IT-ansvarig funktion omedelbart informeras om omständigheterna. Vid stöld av fysisk utrustning tillhörande arbetsgivaren eller som används av den anställde, skall detta utan fördröjning anmälas till polismyndigheten. Elektroniska kort såsom kreditkort, passerkort och mobiltelefonkort (t ex SIM-kort) samt mobiltelefoner skall utan fördröjning spärras hos utfärdande instans eller företag, alternativt operatör.

Bärbara och portabla datorer och mobiltelefoner måste stängas av eller lösenordskyddas om de lämnas utan tillsyn.

4 Funktion och användning

Arbetsgivaren tillhandahåller IT-verktyg till den anställde. Den anställde använder dessa IT-verktyg i sitt arbete. För användning gäller följande:

- Arbetsgivarens IT-verktyg får inte användas på ett sätt som innebär att användaren av IT-verktyget eller arbetsgivaren bryter mot lagar.
- IT-verktyg är ett arbetsverktyg och får för privat bruk användas bara i sådan omfattning att det inte inkräktar på arbetet eller medför onödiga kostnader för arbetsgivaren.
- Ingen utrustning, annan än den som är tillhandahållen av arbetsgivaren, får anslutas till arbetsgivarens nätverk, internetförbindelse, skrivare eller informationssystem, utan arbetsgivarens godkännande.

- Den anställde får installera mjukvara och tillägg till mjukvara (s k ”plug-ins” eller ”insticksprogram”) i arbetsgivarens utrustning *efter* medgivande från IT-ansvarig funktion.
- Om den anställde upptäcker eller blir meddelad om ett virusangrepp eller dokument infekterat av virus så skall IT-ansvarig funktion snarast informeras om detta.
- Informera även IT-ansvarig funktion vid upptäckt av s.k. ”trojaner”, ”spyware” och andra program som har till uppgift att hindra normal användning av IT-verktyg och/eller läcka information till tredje part.
- Vid nyttjande av arbetsgivarens IT-system från en extern plats såsom hemarbetsplats, publik eller extern arbetsplats (t ex publikt nätverkt) eller annat företags IT-verktyg, är det den anställdes ansvar att upprätthålla en tillräckligt hög nivå av informationssäkerhet för att skydda arbetsgivarens information och kommunikation.

Den anställdes e-postadress(er) som tillhandahålls av arbetsgivaren skall i första hand användas för arbetsrelaterad kommunikation. Den anställde bör undvika publicering av arbetsgivarens e-postadresser i media eller forum som inte är arbetsrelaterade. Arbetsgivarens e-postfunktion får utnyttjas för enklare privata ärenden på samma sätt som en tjänstetelefon.

Om den anställde uppfattar eller vill påvisa brister i dessa IT-verktyg, skall detta ske genom att den anställde meddelar IT-ansvarig funktion.

Webbaserade system görs tillgängliga via arbetsgivarens säkerhetsportal HAG. Genom koppling till Active Directory görs efter inloggning bara de system synliga i HAG som den anställde har behörighet till. För vissa system krävs ytterligare en inloggning.

Det är otillåtet att utan tillstånd:

- Försöka tränga igenom interna eller externa säkerhetsspärrar.
- Låta annan anställd, anhörig eller bekant låna lösenord och användarnamn.
- Låta anhörig eller bekant låna arbetsgivarens IT-utrustning.
- Koppla in extern IT-utrustning i arbetsgivarens nät.
- Kopiera eller arkivera exempelvis medlemsregister från arbetsgivarens IT-system.

4.1 Granskning dvs. tillgång till användares användning av IT-system

Arbetsgivaren skall vid behov, ha tillgång till den anställdes e-postkommunikation. Sådant behov *kan* exempelvis motiveras vid anställningens upphörande eller vid säkerhetsintrång i arbetsgivarens IT-verktyg eller IT-miljö.

Den anställde informeras härmed om att arbetsgivaren kan komma att granska spårdata såsom loggfiler och övervakningssystem, som ett led i att förbättra den tekniska plattformen (informationssäkerhet, prestanda, mm) samt att granska att IT-policyn efterlevs. Sådan granskning som kan ske slumpmässigt, vid misstanke om brott och på förekommen anledning, kan innebära att arbetsgivaren identifierar den anställde i kommunikationssammanhang och innehållet i dennes kommunikation. Spårdata såsom loggfiler och övervakningssystem kan komma att sparas i upp till 24 månader.

Den anställde får inte försvåra åtkomst till IT-verktyg för arbetsgivaren genom kryptering eller särskilt lösenordsskydd.

Om det vid granskning framkommer att regler i IT-policyn överträtts kan ärendet komma att utredas av arbetsgivaren. Arbetsgivaren kommer i första hand att sträva efter rättelse genom påpekanden och dialog med den anställde. Vid allvarligare eller upprepade överträdelser kan arbetsgivaren komma att behöva överväga andra åtgärder såsom erinran om att följa skyldigheter som följer med anställningen. I de fall bättring inte sker, kan arbetsgivaren behöva pröva frågan om anställningen kan bestå dvs. grund för uppsägning kan komma att föreligga.

4.2 Användning av e-post och Internet

IT-systemen inom partiet är anpassade efter de krav som verksamheten ställer på funktionalitet och dimensionering. Då den anställde använder Internet eller e-post skall sunt förnuft råda då elektroniska spår lämnas på exempelvis besökta sajter. Detta är av stor vikt då detta arbete utförs i Moderaternas namn. Detta gäller för användningen:

- Att all utgående e-post från Moderaternas domän (@moderat.se) uppfattas som arbetsgivarens då Moderaterna står som avsändare. Att skicka e-post privat från Moderate-postadressen innebär i princip detsamma som att använda Moderaternas brevpapper för privat bruk.

- Den e-post som skickas till Moderaterna (@moderat.se) eller finns lagrat i Moderaternas IT-system betraktas som arbetsgivarens egendom.

- Att iaktta försiktighet om e-post med bifogade filer från ej känd avsändare anländer. Tänk på att att fientlig kod ofta sprids via e-post. Kontakta IT-avdelningen om du är osäker.

- Det är otillåtet att läsa andra användares e-post utan dennes medgivande.

- Moderaternas elektroniska adresser(förnamn.efternamn@moderat.se) skall användas med stor försiktighet vid exempelvis e-registreringar. Detta mot bakgrund av den kraftigt ökade risken för SPAM och kapning av användarkonton.

- Avsändaren ansvarar alltid för att säkerhet och sekretess ligger i paritet med det material som skickas. Detta skall naturligtvis beaktas vid försändelse av partihemliga handlingar med e-post.

- Privat användning av e-post är tillåten, men får inte inkräkta på arbetstid, ska ske sparsamt och med gott omdöme.

Rekommendationer och information

Att säkerheten ofta är sämre utanför arbetsgivarens domän och att utan exempelvis ett certifikat går det inte att säkerställa en avsändares identitet. Det går heller inte att säkerställa om e-brevet har manipulerats eller ej.

Att överväga om känslig information istället bör skickas med vanlig postgång. Detta på grund av att risken för att en obehörig kan komma över informationen ökar när informationen har lämnat arbetsgivarens domän (@moderat.se).

Att undvika överbelastning av e-postsystemen genom att inte skicka onödig information med e-post. Använd istället arbetsgivarens Intranät för material av allmän karaktär.

E-post får aldrig användas på följande sätt inom Moderaterna:

- Till försändelse av e-post för personlig ekonomisk vinning.
- Till försändelse av e-post till någon som tillhandahåller pornografiska produkter.
- Till försändelse av e-post av kedjebrevskaraktär.
- För vidarebefordran av e-post som avses ovan.

Internetanvändning

Internet skall användas för informationsinsamling i tjänsten, detta innebär att användandet av Internet skall vara yrkesmässig. Internet skall användas av samtliga anställda inom partiet med sunt förnuft och gott omdöme. Arbetsgivaren äger rätt att logga all trafik in och ut på Internet.

Internet får aldrig användas på följande sätt inom Moderaterna:

- För nedladdning av upphovsrättsskyddad musik, filmer, mjukvara eller bilder till arbetsgivarens datorer. Dock kan undantag göras då exempelvis bild- eller ljudmaterial behövs på yrkets vägnar. Under dessa förhållanden skall alltid ett godkännande av närmaste chef inhämtas. (Köpt media omfattas inte av denna regel.)

- För att besöka webbplatser som förknippas med pornografi, rasism eller liknande vars innehåll bedöms som olämpligt. Det gäller också sajter som innehåller någon form av olaglig information. Den som i arbetet, för att göra politisk research, behöver besöka den typen av webbplats ska i förväg informera och inhämta tillstånd från sin chef. Pornografiskt material och kränkande material får ej heller förmedlas via arbetsgivarens IT-verktyg.
- För att ladda ner, installera och använda fildelnings-/filbytarprogram som exempelvis Kazaa, Gnutella, BitTorrent.
- För att spela någon form av spel på arbetstid. Detta gäller alla typer av spel.
- För att delta i chat-grupper med Moderaterna som avsändare om det inte avser arbetet, då oklarhet lätt kan uppstå huruvida man företräder Moderaterna eller ej.

4.3 Sociala medier – riktlinjer

I det politiska arbetet vill arbetsgivaren uppmuntra till ett aktivt deltagande i sociala medier. Sett mot den stora genomslagskraft dessa medier har är det viktigt att vi är välrepresenterade här.

Reglerna för internetanvändning gäller även i sociala medier. Var även diskret när det gäller information som är för internt bruk inom partiet dvs. inte publicerad.

För att underlätta användningen ger vi dig här några bra riktlinjer ur arbetsgivarens folder **Netikett** från 2010:

1. Moderaterna söker alltid information i öppna källor. Vi ska aldrig försöka komma åt information som användaren inte vill att vi ska ta del av.

2. Var öppen med din identitet. Om du är dig själv och skriver från dina egna tankar och värderingar så har du störst chans att hamna i diskussion med andra människor som du finner intressanta.

3. Allt du gör på nätet kan spåras och det mesta blir kvar för lång tid. Gör inte något idag som du inte kan stå för även i framtiden.

4. Tänk på att upphovsrätten gäller även på nätet. Upphovsrätten ska respekteras. Be därför alltid om tillstånd om du vill kopiera eller använda program, text, bild, video eller ljud som någon annan har skapat eller innehar rättigheterna till och det inte klart framgår att de är fria att använda. Använd inte heller någon annans fotografi/ bild utan tillstånd från denne.

5. Om du bloggar – var generös med länkningar och hänvisa varifrån du fått fakta och uppgifter.

6. Svara på frågor

7. Spamma inte med för många inlägg om det du tänkt skriva redan har skrivits av dig eller någon annan i samma forum eller e-postlista. Undvik att skicka kedjebrev vidare.

8. Om du är tveksam till om du verkligen ska skriva något – tänk över det en gång till och bolla gärna med någon annan person.

9. Se hur andra gör när du är ny på ett ställe. De flesta kanaler på nätet har sin egen kultur och du kan lära mer av erfarna användare genom att se hur de använder kanalen.

10. Läs FAQ:en först (Frequently Asked Questions) – finns nästan alltid ett dokument i forum och communities med de vanligaste frågorna och förhållningsreglerna. Läs det innan du börjar blogga.

5 Moderaternas medlemssystem

Arbetsgivaren använder ett medlemssystem för att registrera och ajourhålla uppgifter om medlemmar, förtroendevalda, bidragsgivare, prenumeranter och andra intressenter. Systemet används även för att kommunicera med dessa grupper genom olika typer av utskick, centralt, regionalt och lokalt.

Ett antal utvalda personer utgör medlemsadministratörer i systemet. Dessa skall innan behörighet till systemet medges skriftligen underteckna ett tystnadspliktsavtal, samt intyga att man delgivits och förstår innehållet i personuppgiftslagen (PUL).

Medlemsadministratörer ges access till medlemssystemet via säkerhetsportalen FHAG. Efter inloggning i HAG sker ytterligare en inloggning till själva medlemssystemet baserat på individuell behörighetsnivå och roll.

6 Användarkonton

Generellt gäller att alla användarkonton är personliga och skall betraktas som värdehandlingar.

Alla behörigheter är tidsbegränsade och upphör när anställningen, projektdeltagandet eller motsvarande upphör.

Användarkonton (användarnamn och lösenord) som används i partiets interna IT-lösningar får inte användas i externa IT-system så som t.ex. Facebook, Twitter och liknande.

6.1 FirstClass och Intranätet

Arbetsgivaren använder *FirstClass* och dess tillägg *FirstClass Communities* i organisationen. Användarnamn och lösenord väljer man själv i samband med registreringen. Dock skall lösenordet bestå av minst 8 tecken, (inget krav på specialtecken). Lösenordet skall bytas senast efter 100 dagar. De 5 senaste lösenorden sparas och går ej att använda.

Vidaresändning eller omdirigering av e-post till andra mailsystem supporteras inte och utgör en stor säkerhetsrisk. IT-avdelningen ansvarar inte för e-post vilken hanteras på detta sätt. E-post som i samband med vidaresändning/omdirigering försvinner eller ej når tänkt mottagarserver kan ej spåras, återtas eller återskapas av IT-avdelningen när den lämnat arbetsgivarens mailserver (fc.moderat.se).

6.2 Nätverket på Huvudkontoret, Stora Nygatan 30

Alla användare i nätverksdomänen på Stora Nygatan 30 läggs in i Active Directory och tilldelas ett användarnamn och lösenord.
Användarnamnet utgörs av *förnamn.efternamn*

Lösenordet skall bestå av minst 6 tecken, (inget krav på specialtecken).

Lösenordet skall bytas senast efter 100 dagar, därefter låses kontot och användaren ges möjlighet att själv ange nytt lösenord.

De tre senaste lösenorden sparas och går ej att använda.

6.3 Säkerhetskopiering och lagring av data

- Lagring av privata filer på Moderaternas datorer är inte tillåten.
- Lagring av information som är upphovsrättsskyddad (till exempel av Moderaterna ej licensierad programvara, film, musik) på Moderaternas datorer är inte tillåten.
- Användare är skyldig att spara dokument och producerad data i sin hemkatalog alternativt i gemensamma kataloger för respektive avdelning, för att möjliggöra att säkerhetskopiering av datat kan ske.

För information och rekommendationer

Användare som har bärbar dator och som producerar data mobilt (i hemmet, på resa) bör så snart möjlighet ges flytta över datat till sin hemkatalog eller gemensamma kataloger, för att säkra datat.

Säkerhetskopiering av den enskilda användaren på USB-minnen eller annan lagringsmedia, anses ej som en fullgod säkerhetskopiering utan kan istället utgöra en säkerhetsrisk avseende informationsspridning vid ev. borttappat eller stulet lagringsmedia.

Om data lagras på respektive användares arbetsstation (hårddisk på datorn) kan IT-avdelningen ej garantera att datat går att rädda vid ett eventuellt systemhaveri.

Av utrymmesskäl ska kontinuerlig rensning göras. Vid behov av extra stort lagringsutrymme (exempelvis filmat material), kontaktas ansvarig för IT-drift för beslut om val av lämpligt lagringsmedia.

Säkerhetskopiering av hemkatalog och gemensamma kataloger sker varje natt, sju dagar i veckan. Säkerhetskopiering lagras på magnetband som i sin tur alltid lagras ”off-site” ifall något oförutsett med fastigheten skulle inträffa (brand, översvämning, inbrott m.m.).

För hjälp med återskapande av förlorade data i din hemkatalog eller gemensamma kataloger, kontakta IT-avdelningen.

7 Mobiltelefoner och läsplattor

Anställda av partiets riksorganisation förses med en mobil tjänstetelefon. Inloggning på mobiltelefon och i förekommande fall läsplattor, skall ske med användning av låskod. Saknas funktion för särskild låskod skall PIN-kod användas. Denna funktion skall alltid vara aktiv.

Avdelningschef budgeterar för inköp av telefoner, läsplattor, abonnemang samt trafikavgifter för respektive avdelning. Därefter läggs en beställning till IT-avdelningen via support@moderat.se

Beställd utrustning levereras till IT-avdelningen och konfigureras där mot e-postkonto, olika applikationer m.m.. När enheten är klar för användning meddelas användaren och enheten kan då kvitteras ut hos IT-avdelningen.

Användaren registrerar ett eget Apple-ID med privat kontokort. Appar som RO menar ska användas i arbetet och som kostar pengar ersätts enligt principen för kontantutlägg.

Moderaterna har ett ramavtal med operatören Telenor som ger arbetsgivaren ett fastpris på både telefoni och datatrafik.

Några riktlinjer och tips vi användning:

- Tala inte högt om interna partifrågor, på allmänna färdmedel eller då du har främmande människor runt dig som kan avlyssna samtalet.
- Tänk på att den som sitter bredvid dig kan läsa vad du skriver på exempelvis din läsplatta och när du textar ett sms.
- Använd gärna alias på kända personer inom partiet i dina kontakter på telefonen/läsplattan.
- Använd alltid låsfunktionen på din mobiltelefon/läsplatta.

8 Kompetens

- Medarbetare skall ha för arbetsuppgifterna nödvändig kunskap om IT och hur IT skall användas.
- Medarbetare skall erbjudas utbildning för att uppnå den IT-kunskap som krävs för att utföra sina arbetsuppgifter.
- Medarbetare skall erbjudas utbildning där så erfordras för att kunna använda av arbetsgivaren tillhandahållen specifik mjukvara.
- För all medarbetare skall för arbetsuppgifterna nödvändiga IT-kunskaper dokumenteras och utvecklingsplaner skall upprättas. Genomförda utbildningar skall dokumenteras.

9 Utveckling av IT

- Utveckling av IT skall styras av verksamheternas behov.
- IT-tjänster skall utformas för att uppnå en hög grad av användarvänlighet och ge möjlighet till anpassning utifrån den enskilde individens behov.
- IT-tjänster och IT-infrastruktur skall utformas på ett sätt som möjliggör anpassningar till nya och föränderliga krav och behov.
- Vid anskaffning av IT-tjänster skall samordningsvinster och totalkostnad inkluderande kostnader för bland annat drift, underhåll, utbildning, installation och utrustning beaktas.
- Arbetsgivaren skall verka för att anskaffa och etablera gemensamma IT-tjänster, programvarulicenser och standarder såväl inom den egna kansliverksamheten som med fältorganisationen.
- IT-tjänster och IT-infrastruktur skall följa etablerade standarder och ”best practice”.
- Vid val av lösningar/produkter skall, där så är möjligt, tillgängliga/kommersiella väljas före egenutvecklade.

10 Supportorganisation

All IT-support för Riksorganisationens huvudkontor sköts av IT-avdelningen. Alla support-ärenden, förfrågningar och beställningar av konton, behörigheter, IT-utrustning etc. hanteras i arbetsgivarens ärendehanteringssystem.

Felanmälan, frågor och beställningar skickas på e-post till support@moderat.se I samband med detta erhåller anmälare/beställare ett e-postkvitto med ärendenummer. Fortsatt kommunikation i ärendet sker genom att svara på e-postkvittot utan att ändra i ärenderaden. Härigenom bibehålls tråden i ärendet och inget nytt ärendenummer skapas i ärende-hanteringssystemet. IT-avdelningen på St Nygatan 30 är bemannad under kontorstid.

Vid akuta ärenden utanför kontorstid nås IT-chef Anders Gerby på: 073-682 94 44

IT-funktionen har upprättat och ajourhåller en DRP (Disaster Recovery Plan), som möjliggör snabba insatser i samband med större haverier. Moderaternas DRP innehåller bland annat kontaktuppgifter till olika leverantörer, nätverks- och serverbeskrivningar, åtgärdsplaner, checklistor m.m.

11 Miljö

Moderaternas IT-avdelning arbetar aktivt med åtgärder för att minimera den negativa miljöpåverkan som användningen av IT medför. Som ett led i det arbetet försöker vi skapa förutsättningar för alla användare att delta i miljöarbetet genom att följa några enkla regler.

- Stäng av datorn när du går hem för dagen.
- Försök arbeta för att minimera användandet av våra skrivare.
- Inköp av IT-utrustning koordineras och genomförs av IT-avdelningen.
- Uttjänt IT-utrustning lämnas till IT-avdelningen som lämnar det vidare till återvinning.
- Vid val mellan två likvärdiga IT-produkter väljs den med minst skadlig miljöpåverkan.

Moderaterna ska alltid använda bästa tillgängliga metoder i arbetet för att minimera skadlig inverkan av vår verksamhet. Moderaterna strävar också efter ett miljömedvetet beteende hos alla medarbetare och vårt miljöarbete ska regelbundet kommuniceras till våra användare och leverantörer.