Tekniske IT-krav for nye løsninger

Drammensregionen IKT (D-IKT) er et IKT-samarbeid mellom Drammen, Nedre Eiker, Røyken, Sande og Svelvik. D-IKT drifter løsninger for alle våre samarbeidskommuner og interkommunale selskaper (IKS) som helt eller delvis er eid av våre samarbeidskommuner.

Ved anskaffelse av nye løsninger er det nødvendig at løsningene skal fungere godt sammen med de løsningene som allerede finnes og på den tekniske infratrukturen i D-IKT. På bakgrunn av dette har vi laget en liste med krav som de nye løsningene må tilfredsstille.

Innhold

Plattform 1

Virtuelt miljø 1

Databaser 2

Nettverk 2

Autentisering 2

Sikkerhet 2

Integrasjoner 2

Vedlikehold 2

Oppdateringer 2

Plattform

D-IKT har valgt Microsoft Windows servere og klienter som vår primære plattform. Alle nye løsninger som skal installeres på servere og driftes hos oss må kunne kjøre på Windows servere. Alle løsninger må kunne fungere med Windows klienter. Den nye løsningen må fungere på alle versjoner av Windows operativsystemer for server/klient som supporteres av Microsoft.

Virtuelt miljø

D-IKT benytter WMware for virtualisering av servere. Alle nye løsninger som skal installeres på våre servere må kunne kjøre på WMware.

Databaser

D-IKT benytter både Microsoft SQL Server og Oracle databaser. Dersom den nye løsningen benytter databaser som skal driftes hos D-IKT så må det være Microsoft SQL Server eller Oracle databaser. Våre Oracle databaser kjører på IBM AIX. Nye løsninger som benytter databaser og som skal kjøre 24/7 og/eller har særkilte krav til oppetid og ytelse må leveres med SQL Server databaser med støtte for redundans.

Nettverk

Vi benytter Cisco nettverk og Cisco routere. Den nye løsningen må fungere på vårt nettverk og med våre routere. Alle leverandører som skal levere løsninger som skal benyttes i vårt nettverk må forplikte seg til å følge alle datatilsynets retningslinjer for nettverk og sikkerhet. Alle nye løsninger som skal benyttes i våre trådløse nett må støtte autentisering basert på IEEE 802.1x.

Autentisering

D-IKT benytter autentisering basert på bruk av AD (internt), ADFS (eksternt) og FEIDE. Vi benytter dessuten ID-porten for autentisering av innbyggere i våre selvbetjeningsløsninger. Alle nye løsninger må støtte autentisering basert på bruk av ID-porten (for innbyggere), FEIDE (for elever/foresatte) eller AD/ADFS (for elever og ansatte). Dersom den nye løsningen støtter «Single Sign-On» så må den kunne settes opp og konfigureres til å fungere sammen med vår AD/ADFS.

Sikkerhet

D-IKT benytter anerkjente løsninger for å styre datatrafikk inn/ut, unngå søppelpost og hindre skadelig progranvare. Den nye løsningen må fungere sammen med alle anerkjente løsninger for brannmurer, spam og anti-virus.

Integrasjoner

D-IKT benytter mellomvare og integrasjon mellom applikasjoner basert på bruk av web servicer. Effektiv og sikker utveksling av opplysninger mellom løsningene våre forutsetter at de støtter et moderne grensesnitt (API). Dersom den nye løsningen skal utveksle opplysninger med andre løsninger så må den leveres med web servicer med et SOAP API eller et REST API og den må kunne integreres mot andre web servicer med et SOAP API eller et REST API. Utveksling av filer skal skje på XML eller JSON format.

Vedlikehold

Ved behov for vedlikehold av den nye løsningen må leverandøren enten utføre vedlikeholde ved fysisk oppmøte i våre lokaler eller gjennom tilgang utenfra basert på vår VPN. D-IKT tillater ikke at leverandører installerer eller benytter andre løsninger enn vår VPN for tilgang/vedlikehold. Tilgang til vårt nettverk og våre servere forutsetter at alle leverandører og deres ansatte med behov for tilgang signerer en taushetserklæring.

Oppdateringer

Dersom det lanseres nye versjoner av programvare som benyttes i vår tekniske infratruktur, dvs Windows, SQL server, Oracle eller WMware som medfører at den nye løsningen ikke fungerer så skal leverandøren av den nye løsningen kostnadfritt og innen tre måneder levere en oppgradring av sin løsning som fungerer med siste versjon av programvaren i vår tekniske infratruktur. Det samme gjelder dersom det kommer nye versjoner av de løsningene vi benytter for brannmurer, spam og anti-virus.