Informationssikkerhedspolitikken tager højde for følgende krav, strategier og procedurer:

A. Krav fra ISO 27002

B. Nye lovkrav vedr. GDPR
   a. Dataminimering
   b. Protection by design
   c. Databehandleraftaler
   d. DBR (både lovens krav og funktionen i Faxe Kommune)
   e. Godkendelse af nye systemer
   f. Risikovurderinger (risikobaseret tilgang til ALT)
   g. Udvidet dokumentationskrav generelt
   h. Integritet
   i. Registreredes rettigheder
   j. Procedure sikkerhedsbrud

C. Faxe Kommunes nuværende procedurer vedr.
   a. DBR-funktion
   b. Godkendelse af IT-kontrakter og databehandleraftaler
   c. Sikkerhedsbrud

D. Der er inddraget erfaringer fra seneste års samarbejde med IT-revisionen i politikken.

E. Der er taget højde for, at politikken tydeligt understøtter digitaliseringsstrategien.

F. Politikken tager højde for kendte behov/tiltag til forebyggelse af sikkerhedsbrud.

G. Politikken berører i højere grad alle dele af Informationssikkerhedshåndbogen.

H. Ansvaret er præciseret ud fra lovens øgede krav til dokumentation og risikobaseret tilgang.

I. Tilpasset politik på baggrund af Hovedudvalgets høringssvar.

Betydning for medarbejdere:
Politikken understøtter medarbejderne endnu mere end i dag end den gældende politik gør. Det gør den f.eks. ved at beskrive behovet for uddannelse og uddybe ansvaret, så der ikke er tvivl om hvad den enkeltes ansvar betyder og hvilke opgaver det medfører.
Særligt bemærkes, at der er anvendt risikobaseret tilgang i modsætning til i dag, hvor alle forventes at kende hele Informationssikkerhedshåndbogen. Der vil blive taget højde for dette ved udarbejdelse og implementering af håndbogen.
Den eneste skærpelse i forhold til medarbejderne, er at politikken præciserer, at medarbejderne ikke må opbevare private data i Faxe Kommunes systemer. Denne præcisering er indsat på baggrund af den nuværende praksis.