



Informationssäkerhetspolicy

Informationssäkerhetsarbetet på ICU Scandinavia AB har sin utgångspunkt i strukturerade riskanalyser för att avväga rätt skyddsnivå i alla delar av verksamheten för att:

- Konfidentialitet - förhindra eller försvåra för obehöriga att få tillgång till information
- Riktighet - säkerställa att den information som produceras och bearbetas är korrekt, aktuell och fullständig.
- Tillgänglighet - bidra till att informationen är åtkomlig vid behov
- Spårbarhet - säkerställa ursprunget av varje händelse

Detta säkerställer vi genom att:

- säkerställa att anställda, samarbetspartners och leverantörer arbetar i linje med vår informationssäkerhetspolicy med tillhörande riktlinjer och rutiner.
- alla informationstillgångar och teknisk utrustning har tillräckligt skydd.
- ständig kompetensutveckla personalen i handhavande och användning av teknisk utrustning
- utveckla säkra produkter och tjänster
- avvikelser och incidenter systematiskt dokumenteras och följs upp, så att erfarenheter från dessa kan tas till vara som en del av det kontinuerliga förbättringsarbetet
- Identifiera, tolka och uppfylla tillämpliga lagar och andra krav som berör vår verksamhet.

Vårt informationssäkerhetsarbete ska ständigt förbättras med hjälp av kontinuerligt reviderade mål och handlingsprogram.

Denna policy skall omprövas varje gång nya riskanalyser görs.



Information Security Policy

The information security work at ICU Scandinavia AB has its starting point in structured risk analyses to weigh the right level of protection in all parts of the business in order to:

- Confidentiality - prevent unauthorized persons from gaining access to information
- Accuracy - ensure that the information produced and processed is correct, up-to-date and complete
- Availability - contribute to the information being accessible when needed
- Traceability - ensure the origin of each event

We do this by:

- employees, partners and suppliers work in line with our information security policy with associated guidelines and routines.
- all information assets and technical equipment have adequate protection.
- constantly develop the skills of the staff in the handling and use of technical equipment
- develop safe products and services
- deviations and incidents are systematically documented and followed up, so that experiences from these can be used as part of the continuous improvement work
- Identify, interpret and comply with applicable laws and other requirements that affect our business.

Our information security work must be constantly improved with the help of continuously revised goals and action programs.

This policy must be reviewed every time a new risk analysis is done