Utdrag fra ISO/IEC 27002:2022

Informasjonssikkerhet, cybersikkerhet og personvern — Ledelsessystemer for informasjonssikkerhet — Sikkerhetstiltak

Avsnitt 8.13 (engelsk utgave)

8.13 Information backup

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Corrective	#Integrity #Availability	#Recover	#Continuity	#Protection

Control
Backup copies of information, software and systems should be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.

Purpose
To enable recovery from loss of data or systems.

Guidance
A topic-specific policy on backup should be established to address the organization's data retention and information security requirements.

Adequate backup facilities should be provided to ensure that all essential information and software can be recovered following an incident or failure or loss of storage media.

Plans should be developed and implemented for how the organization will back up information, software and systems, to address the topic-specific policy on backup.

When designing a backup plan, the following items should be taken into consideration:

a) producing accurate and complete records of the backup copies and documented restoration procedures;
b) reflecting the business requirements of the organization (e.g. the recovery point objective, see 5.30), the security requirements of the information involved and the criticality of the information to the continued operation of the organization in the extent (e.g. full or differential backup) and frequency of backups;
c) storing the backups in a safe and secure remote location, at a sufficient distance to escape any damage from a disaster at the main site;
d) giving backup information an appropriate level of physical and environmental protection (see Clause 7 and 8.1) consistent with the standards applied at the main site;
e) regularly testing backup media to ensure that they can be relied on for emergency use when necessary. Testing the ability to restore backed-up data onto a test system, not by overwriting the original storage media in case the backup or restoration process fails and causes irreparable data damage or loss;
f) protecting backups by means of encryption according to the identified risks (e.g. in situations where confidentiality is of importance);
g) taking care to ensure that inadvertent data loss is detected before backup is taken.

Operational procedures should monitor the execution of backups and address failures of scheduled backups to ensure completeness of backups according to the topic-specific policy on backups.
Backup measures for individual systems and services should be regularly tested to ensure that they meet the objectives of incident response and business continuity plans (see 5.30). This should be combined with a test of the restoration procedures and checked against the restoration time required by the business continuity plan. In the case of critical systems and services, backup measures should cover all systems information, applications and data necessary to recover the complete system in the event of a disaster.

When the organization uses a cloud service, backup copies of the organization's information, applications and systems in the cloud service environment should be taken. The organization should determine if and how requirements for backup are fulfilled when using the information backup service provided as part of the cloud service.

The retention period for essential business information should be determined, taking into account any requirement for retention of archive copies. The organization should consider the deletion of information (see 8.10) in storage media used for backup once the information's retention period expires and should take into consideration legislation and regulations.

Other information
For further information on storage security including retention consideration, see ISO/IEC 27040.

Avsnitt 8.13 (norsk utgave)

8.13 Sikkerhetskopiering av informasjon

Type sikkerhetstiltak	Informasjons-sikkerhetsegenskaper	Cybersikkerhets-konsepter	Operasjonell kapasitet	Sikkerhets-domener
#Korrigerende	#Integritet #Tilgjengelighet	#Gjenopprette	#Kontinuitet	#Beskyttelse

Sikkerhetstiltak
Sikkerhetskopier av informasjon, programvare og systemer bør vedlikeholdes og testes regelmessig i samsvar med de avtalte temaspesifikke policyene for sikkerhetskopiering.

Formål
Å muliggjøre gjenoppretting etter tap av data eller systemer.

Veiledning
Det bør etableres en temaspesifikk policy for sikkerhetskopiering for å oppfylle organisasjonens krav til dataoppbevaring og informasjonssikkerhet.

Det bør anskaffes tilfredsstillende fasiliteter for sikkerhetskopiering for å sikre at all vesentlig informasjon og programvare kan gjenopprettes etter svikt i eller tap av lagringsmedier.

Det bør utarbeides og implementeres planer for hvordan organisasjonen vil sikkerhetskopiere informasjon, programvare og systemer, for å følge opp den temaspesifikke policyen for sikkerhetskopiering.

Ved utforming av en plan for sikkerhetskopiering bør følgende punkter vurderes:

a) lage nøyaktige og komplette fortegnelser over sikkerhetskopiene og dokumenterte prosedyrer for gjenoppretting;
b) omfanget (f.eks. full eller differensiell sikkerhetskopiering) og hyppigheten av sikkerhetskopiering under hensyn til organisasjonens virksomhetskrav (f.eks. mål for gjenopprettingspunkt, se 5.30), sikkerhetskravene for den involverte informasjonen og informasjonens kritikalitet for organisasjonens fortsatte drift;
c) lagre sikkerhetskopiene eksternt, på et sikkert sted og i tilstrekkelig avstand til at de ikke vil bli skadet ved en eventuell katastrofe på hovedanlegget;
d) gi sikkerhetskopiert informasjon et hensiktsmessig nivå av fysisk og miljømessig beskyttelse (se punkt 7 og 8.1) i samsvar med standardene som gjelder på hovedanlegget;
e) regelmessig teste sikkerhetskopieringsmedier for å være sikker på at de vil være til å stole på hvis det blir nødvendig å bruke dem i nødstilfeller. Teste muligheten til å gjenopprette sikkerhetskopierte data på et testsystem i stedet for å overskrive de opprinnelige lagringsmediene, i tilfelle prosessen for sikkerhetskopiering eller gjenoppretting mislykkes og forårsaker uopprettelig skade på eller tap av data;
f) beskytte sikkerhetskopier ved hjelp av kryptering i henhold til de identifiserte risikoene (f.eks. i situasjoner der konfidensialitet er viktig);
g) sørge for at utilsiktet tap av data oppdages før det tas sikkerhetskopi.

Driftsprosedyrer bør overvåke utførelsen av sikkerhetskopieringer og håndtere feil med planlagte sikkerhetskopieringer for å sikre at sikkerhetskopier er komplette i henhold til den temaspesifikketemaspesifikkepolicyen om sikkerhetskopiering.

Tiltak for sikkerhetskopiering for enkeltsystemer og -tjenester bør testes regelmessig for å sikre at de oppfyller målene med hendelseshåndtering og planer for virksomhetskontinuitet (se 5.30). Dette bør kombineres med en test av prosedyrene for gjenoppretting og kontrolleres mot gjenopprettingstiden som kreves av virksomhetskontinuitetsplanen. Når det gjelder kritiske systemer og tjenester, bør tiltak for sikkerhetskopiering dekke alt av systeminformasjon, applikasjoner og data som er nødvendig for å gjenopprette hele systemet etter en eventuell katastrofe.

Når organisasjonen bruker en skytjeneste, bør det tas sikkerhetskopier av organisasjonens informasjon, applikasjoner og systemer i skytjenestemiljøet. Organisasjonen bør avgjøre om og eventuelt hvordan krav til sikkerhetskopiering skal oppfylles når den bruker sikkerhetskopitjenesten som tilbys som en del av skytjenesten.

Oppbevaringsperioden for vesentlig virksomhetsinformasjon bør fastsettes, under hensyn til eventuelle krav til oppbevaring av arkivkopier. Organisasjonen bør vurdere sletting av informasjon (se 8.10) på pålagringsmedier som brukes til sikkerhetskopiering, når informasjonens oppbevaringsperiode utløper, under hensyn til lover og forskrifter.

Annen informasjon

For mer informasjon om lagringssikkerhet, inkludert oppbevaringshensyn, se NS-EN ISO/IEC 27040.