RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

BACK TO BASICS

IT BACKUP

1/ BUILD AND PROTECT

→ **Define a backup policy** by identifying critical assets for your business and precising the backup frequency for these assets.

→ **Consider backup administration tasks as sensitive operations for your administrators**. These tasks must be protected with relevant measures : dedicated admin workstations, backup flows within a dedicated admin network, etc.

→ **Ensure that your backup infrastructure is not linked with your corporate directories** (e.g. Active Directory) for authentication.

→ **Configure your backup tasks with a fined-grained access control** to guarantee that these backups cannot be modified or altered and are always available, this especially when using a cloud solution.

→ **Be careful with sensitive data backuped to an external site** (public cloud, external providers). Encrypt these data before the backup process and with your own keys, if necessary.

→ **Update your backup infrastructure in a regular way**, in relation with the evolution of your information systems (virtualization, cloud, etc.) and taking into account the continuous threat changes. Do not keep an outdated backup infrastructure in production.

2/ ANTICIPATE AND REACT

→ **Define a restore strategy**, linked with your DRP and the main kill-chain attacks identified for your systems (ransomware, spying, etc.). **Make restore tests regularly**. Involve business leaders on the acceptable downgraded modes in case of cyber-crisis.

→ **Do not forget to include configurations and setup media** of your applications within your backups.

→ **Always make offline backups regularly** (disconnected from all).

→ **Plan to build a process with an emergency button** to isolate your backup infrastructure (servers, media, etc.) in case you suspect a compromission or if you are under a cyber-attack.

→ After an incident, be careful that your backup can contain drivers of compromission. **Restore your systems from trusted sources** (official images, signed binaries), check your configuration files, do an antivirus full scan of your data.

V1.1 (12/23)

www.cyber.gouv.fr / conseil.technique@ssi.gouv.fr