infopulse

Ultimate BCP Checklist_

Are your backups safe?_

01

Is there a risk that a cyberattack can wipe off your assets or damage them? If so, make sure to **guarantee the safety of your backup storages:**

Safe location:

find a place out of reach of cyber criminals that can take advantage of this vulnerability of yours and easily delete or erase your data without adequate permissions.

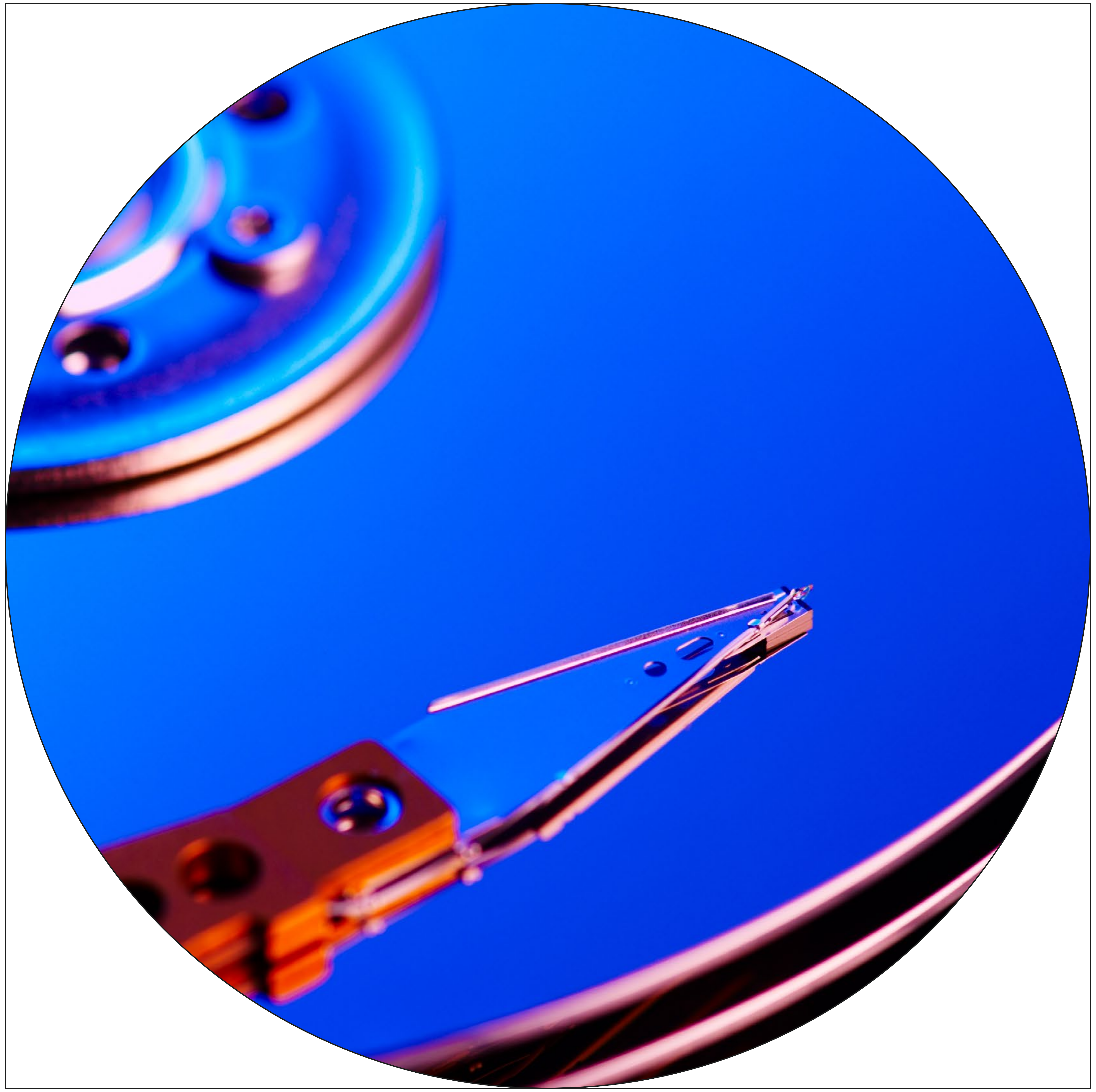
Safe networks:

properly isolate your networks, where backup systems work and store backups.

Safe accounts:

it is a good practice to use separate accounts to maintain backup systems, just not to expose them on daily basis.

Do not forget to conduct security assessments of your backup systems and processes regularly.



Where do you stand with your main website and its backups_

After you safeguarded your main website, attackers can later find a loop and detect backups. Therefore, when working on website protection, you need to verify that your secondary/backup website(s) have the same security level as the main one.

Are your environment parameters in sync?_

03

Usually, policies and security rules contain hardcoded assets. Differences in environment parameters can lower security levels, make security policies work wrong, and give room for malicious attacks. The way out of a potential mishap is automation: use templating, dynamic object names, or scripts. Apply consistent security policies across both primary and secondary (backup) locations, using accurate planning and testing.

The steps to take:

- Deploy and test existing policies looking for possible differences and asset mismatches.
- Review existing access lists and permissions settings.
- Try to simulate the failure of the main website and restore full functionality with backup.
- Conduct security checks for the main and secondary websites.

Can your primary communication channels withstand chaos?_

04

Attackers can shut down your main communication channels, leaving little chance for you to respond proactively. Thus, it gives intruders more time to access system resources and take over the existing controls. What you can do is create backup (or secondary) communication channels for your staff: a communication mechanism for the responsible persons and use it in the case of an infrastructure outage, breach, or any compromise. Preferably, this mechanism should be off-the-infrastructure and not depend on your corporate accounts, infrastructure, or even corporate workstations. Make sure that all response teams can communicate in case the main communication channel is unavailable.

05

Refine your ecosystem security by asking these questions_

1. How does your infrastructure ensure High Availability of services?
2. How do you conduct backup processes? What is your backup plan? How do you ensure consistency? For what period data can be lost? Does your backup plan satisfy the requirements?
3. How do you control timely backups and make sure they are not failing?
4. How do you run your backup/secondary locations?
5. Are there any differences in solutions, performance, or models?
6. How do you distribute configurations between locations?
7. How do you test the security of the same services in different locations?
8. Is your security team capable to monitor the main and secondary/backup locations with the same level of visibility?
9. Do your detection systems cover all sites? Will they detect threats to the secondary site/backup?
10. How do you protect/isolate your backup system/solution?
11. How do you isolate your management plans from main networks?

About Infopulse

Infopulse, part of the leading Nordic digital services company Tietoevry, is an international vendor of services in the areas of Software R&D, Application Management, Cloud & IT Operations, and Cybersecurity to SMEs and Fortune 100 companies across the globe. Founded in 1991, the company has a team of over 2,300 professionals and is represented in 7 countries across Europe and the Americas.

Infopulse is trusted by many established brands, such as BICS, Bosch, British American Tobacco, Credit Agricole, Delta Wilmar, ING Bank, Microsoft, Norwegian Oil and Gas Association, OLX Group, OTP Bank, SAP, UkrSibbank BNP Paribas Group, Vodafone, Zeppelin Group, and others.

For more information, please visit **www.infopulse.com**

Contact us

PL	+48 (663) 248-737
DE	+49 (69) 505-060-4719
US	+1 (888) 339-75-56
UK	+44 (8455) 280-080
FR	+33 (172) 77-04-80
UA	+38 (044) 585-25-00
BG	+359 (876) 92-30-90
BR	+55 (21) 99298-3389

✉ info@infopulse.com