5 STEPS TO ENSURE DATA SECURITY WHILE OUTSOURCING

PREPARED BY ANAKIMS

Even if outsourcing has become a norm for many businesses, you still find that some still step back from doing so because of the security concerns they have. However, if you consider some steps to ensure your data security you need not worry about outsourcing your services, to an outsourcing partner.

Steps to ensure data security

Outsourcing partner should have a standard and strict security policy

When you outsource your service to third party vendor, ensure that they have a standard and secure privacy policy and protection in place, which can also
be considered realistic at the same time. They should have a policy in place for classifying common and sensitive data. Offering standard and fixed guidelines with confirmation from both business managers and information technology professionals of your business, these outsourcing partners will sure keep your sensitive data and idea as secure and protected, as required.

Go with the most suitable service provider

After ensuring that the outsourcing partner has a standard and strict data security policy in place, you will also have to see that they follow through with the policy completely in all their dealings. Having a policy is not enough if the company doesn't deliver to it. They will have to apply these strict security measures, thus ensuring that your data is protected from being copied to other portable devices.

Do not give everyone access to the records

Though easy access to records may ensure smooth functioning of operations, it is better for data security that lesser people within the outsourcing service provider has access to all the records at the same time. Monitor to see if your outsourcing partner follows this rule. Most service providers also educate the employees on how to handle secured and sensitive data.

Ensure that the service provider follows a strict intellectual property policy

See, if the service provider that you plan to outsource your services to follows a strict intellectual property protection laws or privacy policies. Ensure if they monitor the database gateways or the firewalls at the application levels, thus enforcing usage policies and preventing exploitation of vulnerabilities. They would also observe closely the outbound traffic and emails, to avoid any probable data leaks.

The outsourcing partner should employ audits of application and network

If you are looking to ensure that your data is secure, you should look at those service providers that conduct systematic security audits of applications/database and network. This helps them to detect early on the persisting
problems or prospective vulnerability which could cause data leak so that they can rectify it. At the same time, see if the service provider and the employees follow through with any technology to rectify and control the data leak.

Key Takeaway

You can infer from above that following these guidelines while selecting an outsourcing service provider will help you to ensure they have a strict security system in place, thus helping you to curtail any risk of data leak or theft.