6 Data Protection Tips for Universities

When you hear anybody say "knowledge is power," they aren't mistaken in the least. In today's modern world, the right data in the right hands can cause paradigm shifts across entire industries. That's one way to justify the intense measures taken by businesses and institutions to protect their data. Universities are no exception. Being responsible for the futures and welfare of an innumerable population of young people, data protection is a must for universities. Whether it is information about student admission, prospect application, or academic records, to have any of that fall into the wrong hands would be devastating. So here are a few data protection tips that would benefit any university that applies them.

Know Your Risks

Even for an entity like educational institutions, self-awareness goes a long way. To drive that lesson home even further, let us take a look at the 2019 Australian National University data breach as an example. Payroll and personal details that were up to two decades old found themselves into the malicious hands of hackers. The breach affected 200,000 people, with their names, addresses, personal emails, bank details, tax numbers, and academic records all compromised. Since then, many have speculated that the hack was part of an international espionage attempt by the hackers to gain leverage over those from elite families that attended the school.

This chilling example is why universities need to know what data they have and which ones are most vulnerable. For others, what's most at risk can be as simple as the school's log-in details for their social media accounts. A hacked post here and there will seem like nothing compared to the scenario faced by the Australian National University. What administrators can do, for starters, is keep an eye out for avoidable mishaps like using weak passwords or over-relying on automation. Conduct regular evaluations on the systems in place so that checking for irregularities and weak points becomes easier.

Monitor the Flow Continuously

Universities do not stop receiving information. There are always more student records to keep, more payroll for its staff, and more funds to track. It will come to a point where the data flow becomes almost overwhelming, but do not let that discourage you or make you careless. Anything that falls through the cracks can still be valuable to third parties for whatever reason. Stay vigilant and monitor the university's data flow as consistently as possible. With everything accounted for, school administrators will find themselves in

a better position to conduct the proper analysis of what's most at-risk. Submitting a regular report might be an extra challenge to some but it will pay off in the long run.

Encrypt the Sensitive Data

One of the most common data protection methods is the encryption of sensitive data. This is the act of translating data from one form to another, with access granted only to individuals with the decryption key. Universities that decide to employ this method need to take note that even with the level of safety involved, there are still risks. The first thing to remember involves the aforementioned decryption keys.

Like passwords, short or weak keys are easy prey for hackers. This is due to the fact that a common hacking practice is to simply enter characters at random until one guesses the right key. Another risk that needs mitigating is any performance issues created by the involvement of encryption. With that said, now is a good time to mention the myth that any form of encryption automatically affects database performance. In reality, that's only partially true. As long as universities make use of file-level encryption, then database performance is only minimally affected. It is the application-level encryptions that make major dents in the performance.

Educate the Faculty

According to the Ponemon Institute, around 66% of leaders that specialize in data protection believe employees to be the weakest link where data security is concerned. In the case of universities, those would be the faculty. A reliable defense requires everybody's cooperation, which makes additional training a necessity. The training for the faculty may involve keeping everybody up to date with the most recent technology trends, proper use of digital platforms for the purpose of providing high education quality, and basic password security.

Develop Preventive Policies

Like any other organization, a university would benefit from having data loss prevention policies in place. By now it goes without saying that no kind of protection is one hundred percent bulletproof. Yet, by putting certain practices in place, a reliable protection and preventive policy is still within the realm of possibility. A start to these practices was already mentioned above but is worth repeating: identify which data is at risk the most. Remember that this is not just to spare you from any unnecessary waste of time and effort, but it also leads to improved organizational insights.

Besides identifying the data you need to protect, there must also be specific metrics for success in place. Having this can help determine what your return on investment is concerning the policies. There's also the benefit of being able to better determine who efficient your data protection and damage preventive policies are. Other things that university administrators can do is segregate responsibilities amongst themselves and among the trained faculty. Not only will having separate responsibilities prevent any one worker from being spread too thin, but it also helps prevent data misuse.

Invest in the Right Software

Last but not least, if there's any cyber security method that you would want to try, it would be the use of data privacy management software. The choices at your disposal are vast because developers are well aware of the demands for such products. Among the best selections out there include DataGrail, which received the number one spot on G2.com's "Top 4 Data Privacy Management Software" list. Its ease of use and quality of support makes it highly recommendable not only for academic institutions, but also for marketing firms, IT companies, and retail businesses. Other quality software would be SA1360, which came in at number two in the aforementioned list, DPOrganizer, and OneTrust.

International businesses and large corporations are not the only ones with valuable data to protect. Schools have just as much sensitive information to watch over and the tips above will ensure that danger remains far off. Still, one can never be too careful, but with enough vigilance, school administrators and faculty members alike can mitigate the risks without too much hassle.