WinRAR For Educational Institutions

Protection Against Data Leaks

Educational institutions such as schools and universities, are facing new challenges when it comes to data protection and the prevention of data leaks. Everything from grades to teacher evaluations are stored on computers and in the cloud. Teachers and administrators must use their good judgement to implement password protection securely. Anytime data is moved, shared or placed in unprotected storage, it is at risk. Educational institutions are increasingly becoming targets of cyber-attacks, due to the huge amounts of Personally Identifiable Information (PII) they must process. Everything from credit card details, phone numbers, passport numbers and social security information. The impact of a data breach on a school or university can be catastrophic.

Encryption For Educational Institutions

Data encryption makes data unreadable to anyone without the correct encryption key. Encrypted data is referred to a ciphertext and looks like a scrambled mess of letters and numbers to someone who doesn't have the right key to transform it back into readable plaintext.

The use of a strong encryption algorithm, such as FIPs approved, AES 256-bit, protects data files stored at rest, in the cloud and also in transit. It also means that access to the data files for staff and students is secure and easily implemented.

Let's take a look at the various uses data encryption can have in educational institutions:

- TRANSIT

Sending data via email across the internet or within office networks is known as Data In Transit. This data is easily intercepted, meaning it is essential that this data is encrypted before being sent. Typically, this type of encryption is referred to as end-to-end encryption and can be commonly found in many messenger services and email providers.

- AT REST

Documents, emails and other data that is stored on devices is classed as Data At Rest. Huge problems occur when laptops, tablets and smartphones are lost or stolen, because they hold so much sensitive data. Mandatory encryption on these portable devices can help prevent data from being hijacked and also helps educational institutions remain compliant with privacy regulations such as the GDPR.

- FILE LEVEL

To ensure that confidential data is only made accessible to those with the correct encryption key, separately encrypting each file stored on laptops, computers and in the cloud, prevents any accidental file modification. The files remain stored securely and can also be securely shared. Long and difficult passwords should be used, along with a trusted password manager. Administrators should be employed, so that only they have access to password settings and management.

Let WinRAR Help

FIPs approved, AES 256-bit encryption technology is used within WinRAR to add encryption and password protection to archives, making them safe to share and store.

Use WinRAR to make regular backups, keeping sensitive data files up-to-date.

Recover lost or damaged archives with WinRAR's built-in Recovery Record.

With the capacity to store practically any number of files, WinRAR's storage capabilities are enormous.

WinRAR comes with option to time-stamp archives, avoiding unintentional modification or erasure of data.

WinRAR's Admin feature, allows schools and universities to set up controls and limit access to files containing sensitive information.

More than 25 years' experience in the data compression field, with a dedicated and friendly support team.

<- Back to: Industry Sectors

DownloadSupportNewsPartnersIndustryPrivacyContact