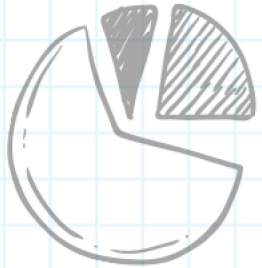
AUGUST 2024 CYBER SECURITY TIP:

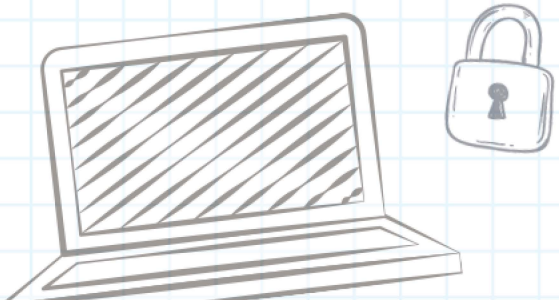
DATA SECURITY



When collecting data, know that you are responsible for maintaining confidentiality, integrity, authenticity, availability and destruction of that data. There are many compliance regulations that must be followed for certain data types.

Know where and how your data is stored, what type of data is being stored and who has access to this data. Do not share or store unnecessary data.

MISSOURI OFFICE OF CYBERSECURITY



Be exceptionally careful when storing and sharing any data. Ask yourself these questions before collecting and sharing data:

- ☐ Does the data need to be collected? If data is not needed, do not collect it.
- ☐ Are there compliance regulations that must be followed with the data being collected? There are many regulatory compliance rules that must be followed for certain data types such as PCI, HIPAA , FERPA, FTI, etc.
- ☐ Is the data being collected and stored in a secure manner? It is best practice to encrypt data at rest and ensure it is stored on a secure device in a secure location.
- ☐ Is data being shared with an authorized resource? Do not share with unauthorized resources.
- ☐ Is data sharing being limited to only necessary content? Do not overshare your data.
- ☐ What type of data is being shared and does it contain sensitive content? Know your data classification and any regulatory compliance rules associated with it.
- ☐ Is the data being shared using safe methods? Use secure methods to encrypt data when it is shared.