Information Security Awareness for New Gadsden State Community College Employees

What is Information Security?

Information Security (InfoSec) is the prevention of unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information.

Please note that InfoSec is concerned with all forms of data, not just electronic data.

_____ (*Please initial here to indicate that you understand the above*)

Why is Gadsden State concerned about Information Security?

Gadsden State is concerned about InfoSec because we recognize the extreme value of the data we are entrusted with. Additionally, we recognize that the modern cyber-landscape is not a friendly place for lax security. We also strive to adopt best practices and be the best stewards of institutional data we can be. Lastly, adequate InfoSec policy and procedures are mandated by the federal government and is essential for Gadsden State to keep Title IV federal financial aid.

_____ (*Please initial here to indicate that you understand the above*)

What type of threats is Gadsden State vulnerable to?

Internally, Gadsden State is vulnerable to threats such as unsecured work areas, unsecured portable devices, and lax enforcement of established policies.

Externally, Gadsden State is vulnerable to threats such as cyber-attacks, malware (spyware, ransomware, etc.), and social engineering.

_____ (*Please initial here to indicate that you understand the above*)

What is Social Engineering?

Social Engineering involves the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

Social Engineering is viewed as a major threat to InfoSec at Gadsden State. To protect yourself, and Gadsden State, from social engineering remember the following:

1. Stay aware and educate yourself. The most important step you can take is to keep yourself educated about different types of social engineering threats. Participate in InfoSec-related professional development and other InfoSec related presentations.
2. Determine if the person requesting information from you is authorized to have access to that information. A common tactic is to put someone on the spot by creating a sense of urgency or importance. Know that the ITS Helpdesk will never contact you to ask for any passwords. Also,

do not respond to any unsolicited emails asking you to update your login information. The Gadsden State Information Technology Services department will never call, or send out an email, asking for login information. In the rare occurrence that the College should ever have to ask you to divulge Gadsden State credentials, it is a requirement that you **must** confirm the legitimacy of the request with your direct supervisor.

3. Understand that you have a responsibility for the data you use. As a steward of GSCC data, you are responsible for the data you handle in your day-to-day duties. You must ensure that any data you are entrusted with remains secure.

_____ (*Please initial here to indicate that you understand the above*)

What do I do if there is a data breach?

Data breaches must be reported.

Any known or suspected data breach must be reported to the GSCC information security assurance team to initiate an appropriate investigation. The preferred method is to email infosec@gadsdenstate.edu. A response will be sent confirming receipt of the notice. During normal business hours, the incident may alternatively be reported to the IT Help Desk by calling 256-549-8341.

It is in your best interest to report a data breach even if you are at fault. The damage from a data breach can be mitigated much more easily if little time has passed. The longer the data has been exposed the harder it is to determine who has accessed the data.

_____ (*Please initial here to indicate that you understand the above*)

What is my part in InfoSec?

1. Educate yourself and stay aware of threats to InfoSec.
2. Comply with existing policy (some relevant policies found in the employee handbook are; F-8.3 Computer Use and Internet Access, M-1.11 Sensitive Data Policy, and M-1.12 Data Breach Policy).
3. Be aware that Gadsden State is involved in an ongoing process to define and refine policies and procedures related to Information Security. Changes to our processes may occur at any time. Your cooperation is appreciated, and required.

_____ (*Please initial here to indicate that you understand the above*)

I acknowledge I have read and understand this Information Security Awareness document

Signature _____ Date _____