REQUESTING ACCESS TO A FORMSTACK FORM FOLDER:

Contact ITech at 601-266-HELP or enter a **work order** to obtain assistance if you do not have access to Formstack or need a new folder. After submitting your work order, please review PII Formstack Process below and complete the **Formstack Privacy Policy Form** to verify your understanding of your responsibilities in the use of Formstack. You are required to complete this form to obtain access to Formstack. The use of a generic (group) email for access to this product is not available.

USER RESPONSIBILITIES: PII FORMSTACK PROCESS

As a user with access to the Formstack software, you are responsible for the proper handling of any data that you might collect. Student workers have the same responsibilities as other account holders. Each user must review and complete the Formstack Privacy Policy Form.

NOTE: Regardless of the number of Formstack folders to which an individual obtains access, each individual only has to complete this process once.

IMPORTANT INFORMATION ABOUT PRIVACY AND FORMSTACK:

The University of Southern Mississippi ("USM") uses Formstack for the creation of forms by groups across campus. Formstack does offer field level data encryption for transmission and storage of private data, which is necessary to protect PII data.

WHAT IS PII? PII is considered sensitive information that can be used, either alone or in conjunction with other information (i.e. data combinations), to identify a specific individual. Examples of this sensitive information that must be encrypted include:

- Data covered under **FERPA**, including GPA.
- Data covered under **HIPAA**

- Date of Birth
- Social Security Number
- Credit/debit card numbers and bank account/routing numbers
- Data Combinations that Result in PII: When certain combinations (i.e. data combinations) of data are collected they rise to the level of information needed to identify a specific individual.

Users of Formstack should not collect any of the following data combinations unless encryption is used to the degree necessary to protect the data being collected.

Combination #1: Name or emplID or email + Social security Number
Combination #2:Name or EmplID or email + driver's license
Combination #3:Number/state ID number (name or emplID or email) +Alien registration number (name or EmplID ID or email) + tax ID (name or emplID or email + passport number
Combination #4:Name or emplID or email + Medicaid Account
Combination #5:Number (name or emplID or email) + full birth date (month/year ok) (name or emplID or email) + mother's maiden name
Combination #6: Any bank account number (with or without a name)
Combination #7:Any credit card number (with or without a name)

NOTE: Since budget strings do not include PII of a sensitive nature, you may collect them.

Recommendations:

If you have any forms in existence that have collected data that falls within one of the data combinations listed above, follow these steps:

- change the status of the form to conditional then disable.
- download the spreadsheet of data collected and then delete the fields that contain the data combination; and
- update the form to remove the data fields that are collecting data that falls within the data combinations.
- Avoid asking for a specific student GPA by allowing the student to select from a GPA range or to answer yes/no that his/her GPA is above a certain value.

- Avoid asking for an individual's entire birthdate (mm/dd/yy). Instead, ask for a birth range or birth month.

HOW TO COMPLY WITH FORMSTACK's POLICY:

You **must** enable data encryption if you are collecting sensitive data such as credit card or social security numbers and storing them in your Formstack database. If you do not do this, you are violating Formstack terms of service and your data is NOT secure.

Tip: For more information on what is and isn't considered sensitive data, check out our Sensitive Data Help Guide!

When you set up your form to save data for later downloading and viewing, you can set a password to encrypt the data when stored in the Formstack database. When you set a password, public and private keys are generated and stored with your form. The public key is used to encrypt the data when saved in the database.

Your password encrypts the private key, which will be used to decrypt the data. Your encryption password is not saved on the server in plain text, so it's not possible for anyone to decrypt the information without knowing your encryption password.

It is important to memorize your encryption password. Neither the vendor nor iTech will be able to retrieve this password for you if lost or unknown - that's how secure this feature is!

Notes:

- *File attachments are not encrypted; however, only those with the associated file upload URL can view the files.*

- *If you are using notification emails and your form has sensitive data in it you must set up the email to either send a link to the database, write a custom message without the sensitive information, or turn on PGP email encryption.*

WARNING: It is important that you memorize or store this password in a safe place. **If you lose this password, we will not be able to retrieve your data, which will be irrevocably lost.**

QUESTIONS:
Please direct questions-

- Regarding Formstack functionality to **forms@usm.edu**.
- To request access, enter a **work order**.
- Regarding forms that must have a payment option to the iTech Help Desk, **helpdesk@usm.edu** and ask about Cashnet, the online payment solution that USM uses.