Customer data security is our #1 priority. We hold ourselves to strict standards and expect our clients to uphold their end of data security best practices. This includes taking extra precautions when passing data back and forth. We ask our clients to abide by these best practices, too.

Best practices for data security:

Never send PII ("Personally Identifiable Information") or Credentials via email.

- Use a screen-grabbing tool such a Greenshot to obfuscate PII

AscentID	First Name	Last Name	Email	Line Item Price	Store
5135872				$399.99	52
3893726				$1,768.50	92
1651580				$99.99	52
2409434				$502.99	33

- If you have a file with PII in it, please upload it to File Manager. Never send the file in an email or ticket.
- Examples of PII include but are not limited to:
  - Names, particularly when paired with data below
  - Postal Address, Email Address, Phone Number
  - Birthday or other Demographic data
- For sending us API Tokens, API Keys, or other necessary credentials, please use a secure note, such as **PrivNote**. Read more here.

Verify before you click.

- If you receive an email that you think is from us, please verify the sending domain.
- When in doubt, reach out to our helpdesk (support@ascent360.com) for assistance. We will do the same – we'll reach out to you if we are ever uncertain about a request.

Audit who has access to your account.

- Set a calendar reminder to do this quarterly.
- If you have personnel changes, please reach out and update us.
- Try to limit who has access to your account and do not share passwords. Reach out to our help desk if you need users disabled.

Finally, a note on "Password Reset" requests.

- We've updated our policy for password resets and will never send a new password (even via PrivNote) via email or a ticket.

- Users will need to reset their password via the “Forgot Password” email that is sent to the email address associated with the account.

If you ever have a question or concern about data security, please contact us.