INFORMATION SECURITY REMINDERS

CARE FOR YOUR CREDENTIALS

✓

- Always change default passwords.
- Use two-factor authentication whenever possible.
- Use unique and strong passwords and change them regularly.

✗

- Do not store passwords in files.
- Do not use your Accenture credentials for personal accounts.

USE APPROVED SOLUTIONS APPROPRIATELY

✓

- Keep security software enabled and restart computers regularly to keep software current.

✗

- Do not put sensitive data on personal devices or in consumer cloud solutions.
- Do not e-mail sensitive data to personal e-mail accounts.
- Do not upload work products to public sites.
- Do not store or transmit sensitive Accenture internal information via client systems.
- Do not circumvent security controls on Accenture workstations.

DEFEND OUR DELIVERABLES

✓

- Verify that users who have access to your work products have a business need.
- Confirm that Accenture has the right to re-use deliverables or deliverable templates.
- And even if we are permitted to reuse deliverables, we can never share client data. You must remove all logos, identifying features from documents, and client data, including hidden sheets, etc.
- When you roll off a project, only keep deliverables and templates that Accenture is permitted to keep and always delete or return all client data in your possession.
- Confirm intended e-mail recipients and correct attachments before sending sensitive information.

✗

- You should never have client data from previous clients stored on your laptop or in your OneDrive for Business folder.
- Do not keep any deliverables when leaving Accenture.

SPOT SOCIAL ENGINEERING

✓

- Review all e-mails for phishing indicators and verify authenticity.
- Use the Report Phishing button to report anything suspicious.
- Look for the [EXTERNAL] tag and pay extra attention because the e-mail is coming from outside the Accenture domain and could be a threat.
- Only open expected attachments from known senders.
- Review hyperlinks to ensure they are overwritten by Proofpoint or direct you to reputable websites.
- Think before responding to any external survey.

ℹ

- Remember, the look of messages sent by Accenture has changed. Colored ribbons may appear if the e-mail is suspicious.

ALERT ASOC IMMEDIATELY

- Call Accenture Security Operations Center (ASOC) immediately at +1 202 728 0645 if you experience a cyber or personal security incident.