Information Security Controls for Exits
Q&A for departing employees

What happens to my access to Accenture systems and data as I get ready to leave the company?

- ❑ We carefully manage your access to ensure we uphold data security practices that are important our clients and our business overall
- ❑ Controls will be applied to your account that will limit your access to sites containing Accenture's and its client's proprietary information and will prevent the download of information to personal devices or accounts. In addition, controls for preventing potential data loss through desktop email clients and personal webmail will be applied
- ❑ **You will still be able to access most Accenture tools and applications from your Accenture-managed or authorized device**

How will this impact me? What accesses will be limited?

You will **no longer be able to**:

- ❑ Access personal webmail (i.e., Gmail, Yahoo Mail, etc.) in the browser, **unless utilizing the ProofPoint Email Isolation Browser.**
- ❑ Access Windows Mail application on Accenture workstation. Outlook should be used as your primary work email application
- ❑ Email attachments to personal email account (gmail.com, hotmail.com, etc.)
- ❑ Send email from Accenture domain to non-Accenture domains (e.g. clients or vendors)
- ❑ Upload, backup, or sync to personal storage sites (Box.com, DropBox, iCloud, Google Drive, etc) or write to USB **(2)**

- ❑ Access the Knowledge Exchange
- ❑ From non-managed or unauthorized devices, you will not be able to access Accenture internal collaboration tools (OneDrive, Teams, Web-email, SharePoint, etc) or Restricted applications (e.g.: SAP)
- ❑ Access CyberArk (PAM.accenture.com) and Administrative accounts
- ❑ Access to sensitive business apps (i.e., SAP BR, MMS, MMB, MME, MMC, Insights MP)

(1) Excludes following countries: Belgium, Costa Rica, Finland, France, Germany, Israel, Kazakhstan, Luxembourg, Qatar, Sri Lanka, Turkey (DLP not legally approved for leavers)

(2) We fully understand that you may have some personal files on your Accenture device – see below for a step-by-step guide on how to transfer them

How do I transfer personal files from my Accenture device?

- ❑ Policy 57 reminds employees to make sure that personal devices are used for non-business-related matters such as sending personal emails, saving non-work-related documents or information such as credit card statements and family photos.
- ❑ Similarly, any work products created to serve a business purpose are not considered personal but proprietary to Accenture or its clients
- ❑ To get a copy of your employment personal files such as Payslip, BIR 2316, Contribution Certificates, etc. to be sent to your personal email address, send the request via ExitManagementQuery@accenture.com.

How do I access my personal webmail (e.g.: Gmail, Yahoo Mail) from my Accenture device?

- ❑ You will be able to access your personal webmail through the Proofpoint Email Isolation browser instead of your regular internet browser
- ❑ The Isolation Browser blocks the ability to upload and download attachments to and from your personal webmail. Viewing and printing attachments is enabled
- ❑ Visit the Proofpoint Email Isolation Browser support site for instructions on how to register and use the browser, as well as Frequently Asked Questions.

What if I need my access back for business or client delivery purposes, or if the process outlined above to remove personal files is not adequate?

- ❑ An exception process has been implemented to request access reinstatement if needed for business purposes or if additional data transfer capabilities are required. Additional approvers may be needed based on the request type. Note that once requested/approved, it will take 6-8 hours for your access to be fully restored for the designated period for the type of exception.
- ❑ To **submit an exception request** or for additional details, visit this site: https://ts.accenture.com/sites/HR_Information_Security_Access_Exceptions/SitePages/Home.aspx

Who can I contact for additional inquiries on these controls and processes defined above?

- ❑ Please contact your HR Partner, Exit case manager or send your inquiry to HR.EnablementCenter related to blocks mentioned on this material. The HR Enablement Center will provide a response within 24 hours (except weekends).

Your Data Privacy

The protection of your personal data is very important to Accenture. Accenture is committed to keeping your personal data secure and processing it in accordance with applicable data protection laws and our internal policies, including Accenture's Global Data Privacy Policy 90.

Accenture invites you to carefully read its privacy statement, which includes important information on why and how Accenture is processing your personal data.

These additional steps for departing individuals are for information security and data protection purposes, in accordance with applicable laws and internal policies, in particular Accenture Policy 57.