WHAT IS DEVX?

- A cloud-based Research & Development ecosystem providing environments & capabilities that enable rapid prototyping, innovation & fast-paced development of POCs, prototypes.
  - NOTE: DevX is isolated from DTCC Network per agreement with Technical Risk Mgmt.
  - DevX Cloud Environment, Tools, and Applications cannot be accessed from DTCC Laptops / VDI and DTCC Network
  - Only White Data can be hosted on DevX
- What's offered
  - POC spaces are isolated from each other
  - Single Sign On using Entra ID, with MFA
  - JIRA for project management
  - Confluence for product documentation
  - White Data transfer process after approvals
  - Artifacts (say, code) ingestion process, post POC completion

DEVX ECOSYSTEM - ONBOARDING GUIDELINES

- **The permissions on DevX are generally very broad to allow you develop your POC unrestricted but with reasonable security in mind.**
  - You will also be required to acknowledge receiving, reading and understanding the Rules of Engagement document (this document).
  - Upon your acknowledgement, we will provision your SSO access to DevX. SSO requires you to setup MFA, Microsoft Authenticator on your phone.
- **Dev Tools**: For POC/Prototype delivery, team can take advantage of Jira – Project Management, and Confluence - Product Documentation. Please check with **support@devx.systems** for more information. DevX team will guide you on accessing these utilizing your SSO.

DEVX ECOSYSTEM – RULES OF ENGAGEMENT

- Consistent naming standards for each Cloud resource must be followed.
  - Each resource name must be prefix with business unit name.
  - Each resource must be tagged. Non-tagged resources will be removed without any prior notice.
- **Must NOT use the terms "dtcc" or "dtcc.com" in any resource creations (including DNS entries) on DevX.**
- Must remove/shutdown/terminate unwanted/old/stale resources on a regular basis.
- Actively protect resources from cyber attacks, software vulnerabilities and license legalities. For example, 1) the internet facing EC2/VM instances should not allow wide-open (0.0.0.0/0) ingress rules, 2) Installed software must be upgraded to fix the vulnerabilities, 3) Review FOSS / COTS licenses carefully before installing software.
- AWS Environment only - Actively monitor GuardDuty, Config Rules, Trusted Advisor findings and Cost Explorer Reports. For each team's convenience, these notifications will be sent to project leads.
- ONLY USE WHAT YOU NEED. Cloud resources can be spun up easily, use best judgement in determining the size and capacity of the resources you need to keep costs down.
- Only White data is allowed on DevX.