

# Access Credentials Compliance Policy

## Policy Statement:

All Employees are responsible for safeguarding their system access including but not limited to **Login/G-Suite/Skype/Medflow/HRM ID/ Settlement Portal** passwords and credentials and must comply with the password parameters and standards identified in this policy. Passwords must not be shared with or made available to anyone in any manner that is not consistent with this policy and procedure.

Credentials including login ids and passwords cannot be shared with anyone not even to another employee, the department manager, directors, COO and CEO.

## Scope of the Policy:

Assigning unique user logins and requiring password protection is one of several primary safeguards employed to restrict access to the Appedology/Proglobal Technologies Network and the data stored within it to only authorized users. If a password is compromised, access to information systems can be obtained by an unauthorized individual, either inadvertently or maliciously. Every employee is responsible for safeguarding against unauthorized access to their account, and as such, must follow to this policy in order to ensure passwords are kept confidential and are designed to be complex and difficult to breach.

## Usage of Credentials:

The credentials which are generated from the IT, HR department should be shared with the concerned employee only, and the employee is responsible for keeping it classified and should only be in their possession. Credentials are shared with employees via email.

Categories of Credentials:

- **HRM ID**
- **G-Suite Account**
- **Settlement Portal**
- **Medflow (KHI/IWP/Accounts/PI)**
- **DOMAIN ID**
- **Skype ID**
- **Client Portals**
- **Project Management Software**
- **Company's paid/unpaid accounts of various/all software's**

## Sharing credentials with others

Sharing the credentials with another employee is strictly prohibited, if shared for what so ever reason will immediately result in termination of the employee.