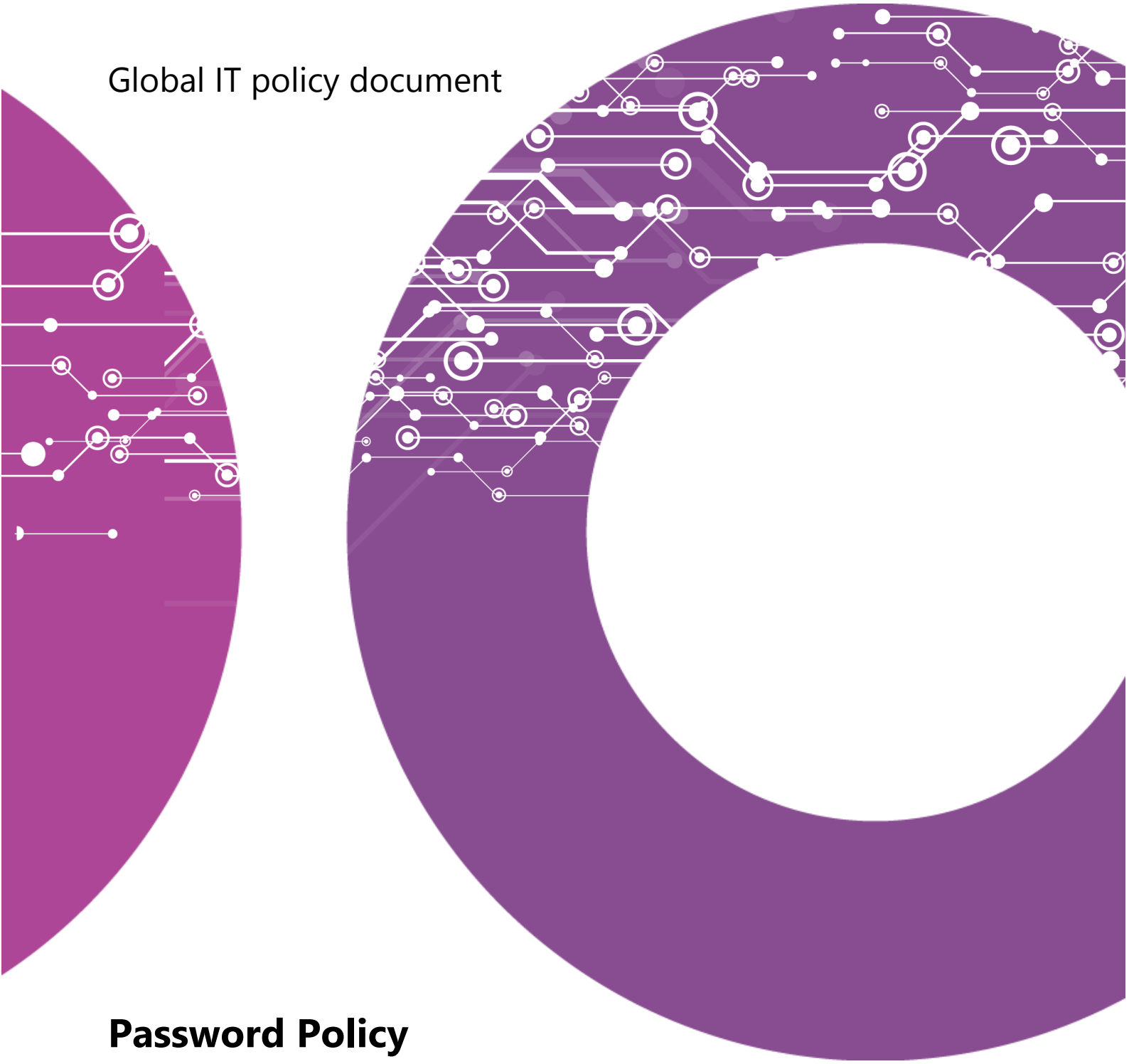
Global IT policy document



Password Policy

GIT-PLD-100006
Revision 1, 2 October 2018

The purpose of this policy is to establish the rules and requirements for creation, storage, protection, and use of passwords in the Wood environment. These requirements are designed to minimize the potential exposure to Wood from damage which may result from unauthorised use of Wood resources.

Revision history

Document Owner:	Malcolm Norman, Director IT, Security & Risk
Document Approver(s):	Jodi Roberson, Director IT, Strategy & Governance
Document Checker:	Judith Ballantyne, Strategy & Governance Analyst
Document Author:	Andrew Thom, Business Information Security Officer
Responsible Party:	The functional responsibility for the development, review and maintenance of this document rests with IT Security & Risk.
Application:	Global.
Storage Location:	Management system.
Revision No.:	1
Effective Date:	2 October 2018
Revision History:	Rev 1, 2 October 2018, updated bullet point relating to password sharing with authorised personnel Rev 0, 19 July 2018, initial issue for use.

Contents

1.0 Scope

This policy applies to all employees, contractors, third-parties, or other agents (hereafter referred to as "users") who have or are responsible for an account (or any form of access that supports or requires a password) on any devices with access to the network or Wood non-public information.

2.0 Policy requirements

When using an account to access any Wood information, users are responsible for preventing any access to any Wood computer resources or data from non-authorised use.

Users must immediately report any suspected compromises via the IT Service Center. Any accounts suspected of compromise will have the associated passwords immediately reset.

The following requirements apply to any and all passwords used to access Wood's network or non-public information:

- All user and system-level passwords must conform to the password construction standard. Passwords should be constructed to not be easily guessed such as use of cyclical terms, dictionary terms, or personal information in the password
- System administrators must use the password construction standard to set up the password settings within their respective systems
- The password assigned to an account must be unique to that account. Users must not create or maintain the same password across multiple accounts, including other work accounts or personal accounts
- Privileged accounts and remote users must utilise multi-factor authentication where systemically possible
- Users must change their passwords with regularity, when not systemically enforced
- Users must not reuse previous passwords, when not systemically enforced
- Users are responsible for the protection of their passwords. Users must not share their passwords with unauthorised individuals or parties, write down any passwords, or store passwords in clear-text. Deskside support and IT support teams are considered authorised users when supporting or troubleshooting a user request. All passwords should be treated like sensitive information
- Users with woodplc.com accounts must register and maintain password security in the self-service password reset manager
- Users must not use the "remember password" feature of applications (for example, web browsers)

3.0 Related policies, procedures, processes, and standards

- Password construction standard
- Information security policy
- IT acceptable use policy