POLICY / PROCEDURE			
DESCRIPTION	FRG Policy – Access Control	AUTHOR	FRG Information Security (FRGIS) Team Lead – Chuck Beck
ISSUED TO	FRG Employees and Contractors; External Parties as Applicable	ORIGINAL DATE	October 2018
INFORMATION CLASSIFICATION	Private Information	NEXT PLANNED REVISON DATE	October 2020

FRG POLICY
ACCESS CONTROL

1. PURPOSE

1.1 The purpose of this FRG Policy – Access Control is to control access to information by ensuring authorized user access and preventing unauthorized access to information, information processing facilities and business processes.

2. SCOPE

2.1. This FRG Policy – Access Control applies to FRG employees, contractors, external parties, and lines of business within FRG as required.

2.2. This FRG Policy – Access Control applies to FRG systems, networks, applications, and technology assets owned or operated by FRG as required.

3. ACCESS CONTROL POLICIES

3.1 FRG will define a comprehensive access control policy and procedures based on business and information security requirements.

3.2 The FRGIS Team will ensure that a user registration and de-registration process is implemented to enable assignment of access rights.

3.3 The FRGIS Team will ensure that a user access provisioning process is implemented to assign or revoke access rights for all user types to all systems and services.

3.4 The FRGIS Team will ensure that the allocation and use of privileged access rights is restricted and controlled.

3.5 The FRGIS Team will ensure that the allocation of secret authentication information is controlled through a formal management process.

3.6 The FRGIS Team will ensure that users' access rights are reviewed at regular intervals.

3.7 The FRGIS Team will ensure that that access rights of all FRG employees, contractors and external party users to information and information processing facilities will be removed upon termination of their employment, contract or agreement, or adjusted upon change.

3.8 The FRGIS Team will ensure that access to information and application system functions is restricted in accordance with this FRG Policy – Access Control.

3.9 The FRGIS Team will ensure that where required by this FRG Policy – Access Control, access to systems and applications is controlled by a secure log-on procedure.

3.10 The FRGIS Team will use password management systems that ensure quality passwords.

3.11 The FRGIS Team will ensure that the use of utility programs that might be capable of overriding system and application controls is restricted and tightly controlled.

3.12 The FRGIS Team will provide policies and procedures for clear desk for papers and removable storage media and for clear screen for information processing.

3.13 The FRGIS Team will provide policies and security measures to protect information accessed, processed or stored at teleworking sites.

4. USER RESPONSIBILITIES

4.1 Users including FRG employees, contractors and external parties as required must follow FRG policies and procedures for access to systems, networks, applications, etc. as directed by the FRGIS Team.

4.2 Users including FRG employees, contractors and external parties as required must follow FRG's practices in the use of secret authentication information.

4.3 Users including FRG employees, contractors and external parties as required will only be provided with access to the network and network services that they have been specifically authorized to use.

4.4 Users including FRG employees, contractors and external parties as required must follow the FRG policies and procedures for clear desk for papers and removable storage media and for clear screen for information processing facilities.

4.5 Users including FRG employees, contractors and external parties as required must ensure that unattended equipment has appropriate protection, keeping in mind information classifications and general information security considerations.

4.6 Users including FRG employees, contractors and external parties as required must follow FRG policies and supporting security measures protect information accessed, processed or stored at teleworking sites.

5. ROLES AND RESPONSIBILITIES

5.1 The FRG Policy – Organizing Information Security provides a description of roles that support all FRG information security related policies, including this one.

6 REPORTING EVENTS AND WEAKNESSES

6.1 FRG employees, contractors and external parties as required must report events and weaknesses related to any part of this FRG Policy – Access Control to the FRGIS Team Lead. Definitions of what constitutes an event or weakness and the process to follow are contained in the FRG Policy – Information Security Incident Management.

6.2 FRG employees, contractors and external parties as required have an obligation to actively support the operations of this FRG Policy – Access Control and to assist FRG in meeting the Policy's underlying purposes and improving its function.

7 COMPLIANCE

7.1 FRG employees, contractors and external parties as required must follow this FRG Policy – Access Control.

7.2 The details of compliance for this FRG Policy – Access Control are contained in the FRG Policy – Compliance (Information Security).

8. RELATED INFORMATION

8.1 The following FRG policies are related to information security:

8.1.1 FRG Policy - Access Control
8.1.2 FRG Policy - Asset Management
8.1.3 FRG Policy - Compliance (Information Security)
8.1.4 FRG Policy - Communications and Operations Management (Information Security)
8.1.5 FRG Policy - Business Continuity Management
8.1.6 FRG Policy - External Parties (Information Security)
8.1.7 FRG Policy - Information Systems Acquisition, Development and Maintenance
8.1.8 FRG Policy - Information Security Incident Management
8.1.9 FRG Policy - Organizing Information Security
8.1.10 FRG Policy - Physical and Environmental Security

8.2 The following FRG policies are relevant to ISO 27001 specifically and are in addition to all FRG policies (above) related to information security:

8.2.1 FRG Policy - Information Security Management System (ISMS) Policy and Operating Procedure

8.3 The following documents support this FRG Policy – Access Control:

8.3.1