POLICY / PROCEDURE			
DESCRIPTION	FRG Policy – Compliance (Information Security)	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
COMPLIANCE (INFORMATION SECURITY)

1. PURPOSE

1.1. The purposes of this FRG Policy - Compliance (Information Security) are to provide for consistent compliance policies and procedures for all FRG information security related policies and to avoid breaches of any law, statutory, regulatory or contractual obligations relevant to information security.

2. SCOPE

2.1. This FRG Policy - Compliance (Information Security) applies to FRG employees, contractors, external parties, and lines of business within FRG as required.
2.2. This FRG Policy - Compliance (Information Security) provides for compliance policies and procedures for all FRG information security related policies, including:

2.2.1 FRG Policy - Access Control
2.2.2 FRG Policy - Asset Management
2.2.3 FRG Policy - Compliance (Information Security)
2.2.4 FRG Policy - Communications and Operations Management (Information Security)
2.2.5 FRG Policy - Business Continuity Management
2.2.6 FRG Policy - External Parties (Information Security)
2.2.7 FRG Policy - Information Systems Acquisition, Development and Maintenance
2.2.8 FRG Policy - Information Security Incident Management
2.2.9 FRG Policy - Organizing Information Security

2.2.10 FRG Policy - Physical and Environmental Security
2.2.11 FRG Policy – Information Security Management System (ISMS) Policy and Procedure

2.3 This FRG Policy - Compliance (Information Security) provides for compliance with legal requirements related to information security.

3. COMPLIANCE WITH FRG INFORMATION SECURITY POLICIES

3.1. All suspected violations of any FRG information security related Policy (listed above) should be reported to the FRG Information Security (FRGIS) Team.
3.2. FRG employees and contractors have an obligation to raise any question they may have as to whether there has been a breach of any FRG information security related Policy.
3.3. Reported violations of FRG information security are treated confidentially.
3.4. Potential penalties for any breach of any FRG information security related Policy include disciplinary action up to and including termination, as well as legal action and reporting to authorities where appropriate.
3.5. The FRGIS Team will regularly review compliance to FRG information security related policies and procedures using various methods.
3.6. FRG information systems are subject to review for compliance with FRG information security policies and standards by FRGIS Team as appropriate.
3.7. Managers are expected to ensure that their systems adhere to FRG policies and procedures.
3.8. Any exception to any FRG information security related policy must be approved in writing in advance by the FRGIS Team.

4. COMPLIANCE WITH LEGAL REQUIREMENTS

4.1 The FRGIS Team will identify applicable legislation and contractual requirements relevant to information security, and will define and document FRG's approach to meet these requirements for each information system.
4.2 FRG will ensure appropriate procedures are implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.
4.3 FRG will ensure that policies and procedures are in place to protect records from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislative, regulatory, contractual and business requirements.
4.4 FRG will ensure that policies and procedures are in place to ensure the privacy and to protect personally identifiable information as required in relevant legislation and regulation.

4.5 FRG will ensure cryptographic controls will be used in compliance with all relevant agreements, legislation and regulations.

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 - Compliance (Information Security)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 - Compliance (Information Security) and to assist FRG in meeting the Policy's underlying purposes and improving its function.

7 COMPLIANCE (TO THIS POLICY)

7.1 FRG employees, contractors and external parties as required must follow this 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 - Compliance (Information Security):

8.3.1 FRG Employee Manual