Cyber Security Exceptions Procedure

Section 1 - Purpose and Scope

(1) The University of Queensland (UQ or the University) establishes Cyber Security Standards to ensure that cyber security controls are implemented consistently and comprehensively and to provide a basis for continual improvement. UQ's cyber security standards are subject to rigorous review and approval processes to ensure they meet the business and technical requirements of the University, and are continually improved and updated as UQ's requirements change.

(2) This Procedure supports UQ's Cyber Security Policy by providing the required process for effective management of exceptions to UQ's cyber security standards to mitigate risk and satisfy business requirements at UQ. The Procedure applies to all consumers of UQ's information and communication technology (ICT) resources and systems (UQ consumers) as defined in the Information and Communication Technology Policy.

Context

(3) A Cyber Security Standard is a document setting out a specification, procedure or guideline. The standard should clearly model the outcome it is designed to produce, so that it is relatively easy to determine compliance. The standard may include permissible variations to a general scheme to provide flexibility and accommodate a broad range of situations.

Section 2 - Process and Key Controls

(4) Requests for cyber security exceptions must be made in writing to UQ's Security Architect in accordance with the requirements of this Procedure.

(5) UQ's Security Architect will review all requests for exceptions in consultation with the requester and other key stakeholders and subject matter experts.

(6) Cyber security exceptions must be approved by the Chief Information Officer after considering advice and recommendations from UQ's Security Architect.

(7) An overview of UQ's cyber security exception process is linked in the Appendix.

Section 3 - Key Requirements

Requesting an Exception

(8) Requests for exceptions to cyber security standards must be submitted to UQ's Security Architect (governance@its.uq.edu.au) and contain the following information:

a. a description of the instance;
b. a description of the required exception;
c. the reason the exception is required;

d. how long the exception is needed and a list of actions with time frames to implement compliance before the exception expires; and
e. a completed risk assessment, including a description of an alternative cyber security control (if one is proposed).

Risk Assessment

(9) In accordance with UQ’s Enterprise Risk Management Framework, a request for an exception must include a risk assessment to determine the level of risk that the University is exposed to if the exception is granted. The risk assessment will take into account any alternative cyber security controls that may be applicable to ensure the managed risk level remains within the University's risk appetite.

Criteria for Granting an Exception

(10) Requests for cyber security exceptions will be assessed by UQ’s Security Architect against the following criteria:

a. Any adverse impact of applying the standard and the frequency of similar instances requiring an exception.
b. The length of time the exception is required for.
c. The proposed alternative control to provide acceptable risk mitigation.
d. The net benefit of granting an exception to the standard.

(11) Cyber security exceptions will be granted on a time limited basis only and in alignment with UQ's Enterprise Risk Management Framework and risk appetite statement. Upon expiry of an exception, compliance with the cyber security standard is required or a new exception request must be submitted.

Review and Assessment of Exception Request

(12) UQ’s Security Architect will review the request and assess whether:

a. the request satisfies the criteria for granting an exception;
b. the risk assessment identifies the relevant risks and controls to ensure the managed risk level is within UQ’s risk appetite; and
c. the exception demonstrates a clear benefit to the University.

(13) UQ’s Security Architect will make a recommendation to the Chief Information Officer based on the above assessment.

Approval

(14) The Chief Information Officer will review the recommendation from UQ’s Security Architect and will decide whether to grant or refuse the request for a cyber security exception.

(15) The Information Technology Services Division will advise the requester of the Chief Information Officer's decision.

Cyber Security Exceptions Register

(16) All cyber security exceptions that have been approved by the Chief Information Officer will be recorded in the University’s Cyber Security Exceptions Register, which will be reviewed annually by the UQ Security Architect and the Information Security Group.

Section 4 - Roles, Responsibilities and Accountabilities

UQ Consumers

(17) UQ consumers are responsible for submitting requests for exceptions to UQ's Security Architect in accordance with the process outlined in this Procedure.

UQ Security Architect

(18) The UQ Security Architect is responsible for:

a. Reviewing requests for exceptions in consultation with the requester, relevant stakeholders and subject matter experts.
b. Managing cyber security exceptions including processing requests for exceptions in accordance with this Procedure.
c. Maintaining the Cyber Security Exceptions Register.
d. Ensuring the University's cyber security standards are well maintained.

Chief Information Officer

(19) The Chief Information Officer is responsible for approving exceptions to cyber security standards after considering advice from UQ's Security Architect.

Section 5 - Monitoring, Review and Assurance

(20) The Chief Information Officer will review this Procedure as required to ensure it aligns with UQ's Cyber Security Strategy and industry best practice.

Section 6 - Recording and Reporting

(21) The UQ Security Architect is responsible for reporting annually to the Chief Information Officer on information collected and held in the Cyber Security Exceptions Register.

Section 7 - Appendix

Cyber Security Exception Procedure

(22) The following diagram provides an overview of UQ's cyber security exception process.

> See linked diagram: Cyber Security Exceptions Procedure Process.

Related Policies

(23) Related policies include:

a. Cyber Security Policy

b. Information and Communication Technology Policy.

Status and Details

Status	Current
Effective Date	7th February 2020
Review Date	16th October 2022
Approval Authority	Chief Information Officer
Approval Date	7th February 2020
Expiry Date	Not Applicable
Policy Owner	Rowan Salt Chief Information Officer
Enquiries Contact	Information Technology Services