Information Security - Data Integrity Directive

Section 1 - Overview

(1) This Directive sets out the minimum requirements that all personnel must follow to protect the integrity of information for which we are responsible.

(2) Maintaining the integrity of information is essential to protecting our clients, our business operations and our reputation. Every person who creates, accesses, modifies or deletes information has a responsibility to ensure that information remains complete, accurate and reliable.

Section 2 - Scope

(3) This Directive applies to all personnel who create, access, modify, transmit or delete information or information assets on behalf of the Organisation.

(4) This Directive supports the Information Security Policy.

Section 3 - Directive

(5) When creating, accessing, modifying, transmitting or deleting information, you must:

a. verify that you are working with the correct client, record, file or information before making any changes;
b. ensure that information is entered, updated or otherwise managed accurately and completely;
c. take reasonable steps to verify that changes have been applied correctly before completing the task;
d. not overwrite, replace, delete or otherwise modify information unless authorised to do so and satisfied that the action is correct;
e. preserve information that may be required for legal, contractual, operational or audit purposes;
f. immediately report any actual or suspected incorrect, incomplete, unauthorised or unintended creation, modification, deletion or disclosure of information;
g. cease processing where there is uncertainty regarding the identity of a client, the correctness of information, the record being updated or the action being performed until the matter has been resolved;
h. not use assumptions, estimates or unverified information where its accuracy is material to the task being performed;
i. protect information from accidental loss, corruption or unauthorised modification throughout its lifecycle; and
j. comply with applicable policies, procedures and other directives relating to the management and protection of information.
k. not proceed with any action where you have reason to believe the information, record or intended action is incorrect until the matter has been resolved.

(6) Failure to comply with this Directive may compromise the integrity of information, adversely affect our clients or

business operations, and may result in disciplinary action or other appropriate corrective measures.

Section 4 - Related Documents

(7) Refer to the Information Security Policy.

Section 5 - Definitions

(8) Definitions applicable to this Directive are contained in the Corporate Glossary.

Status and Details

Status	Current
Effective Date	26th June 2026
Review Date	26th December 2028
Approval Authority	Director
Approval Date	26th June 2026
Expiry Date	Not Applicable
Responsible Manager	Joanne Auld Director
Author	Joanne Auld Director
Enquiries Contact	Joanne Auld Director

Glossary Terms and Definitions

"Information Asset" - Means any information, regardless of form or medium, together with the systems, applications, infrastructure, services or components used to create, collect, process, store, transmit, protect or dispose of that information, where the loss, compromise or unavailability of the asset could affect the Organisation or its stakeholders.

"Information" - Means knowledge or data, regardless of form or medium, including electronic, physical, verbal or visual information.