

Table of Contents

- 1. INTRODUCTION 3
- 2. DEFINITIONS AND INTERPRETATION 3
- 3. WHO IS COVERED UNDER THE POLICY 4
- 4. WHAT IS COVERED UNDER THE POLICY 4
- 5. BREACH OF THIS POLICY 5
- 6. REPORT A BREACH OF THIS POLICY 5
- 7. VARIATIONS TO POLICY 5
- 8. AVAILABILITY OF POLICY AND FURTHER INFORMATION 6
- 9. REVIEW OF POLICY 6
- DATA INCIDENT RESPONSE PLAN 7
- 10. OVERVIEW 7
- 11. STEP 1 – IDENTIFYING A DATA BREACH 7
- 12. STEP 2A – INTERNAL NOTIFICATION 8
- 13. STEP 2B – CONTAIN THE BREACH 9
- 14. STEP 3 – INVESTIGATE AND ASSESS THE BREACH 10
- 15. STEP 4 – COMMUNICATIONS 11
- 16. STEP 5 – REPORTING THE BREACH 13
- 17. STEP 6 – POST-INCIDENT REVIEW 14
- 18. WHERE YOU CAN SEEK FURTHER HELP 15
- 19. DOCUMENT CONTROL 15
- SCHEDULE 1 DATA BREACH RESPONSE TEAM 16
- SCHEDULE 2 DATA BREACH RESPONSE CHECKLIST 20
- SCHEDULE 3 DATA BREACH IMPACT SEVERITY ASSESSMENT GUIDE 22
- SCHEDULE 4 POST DATA BREACH REVIEW 25

DISCLAIMER

CCIWA has taken all reasonable care in preparing this Data Breach Policy and Incident Response Plan. The content of this document is provided as a general guide only and is not designed to be comprehensive or to provide legal advice and should not be relied upon as such. CCIWA gives no warranties or assurances that this document is suitable for your intended use. CCIWA, its employees and/or any other person involved in the preparation of this document will not accept any responsibility for any direct, indirect or consequential loss or damage occasioned to any person acting or refraining from acting as a result of material contained in this document, or otherwise in connection with it. We encourage you to contact the Commercial Legal Team at CCIWA if you wish the document to be tailored to suit your particular business or commercial needs.