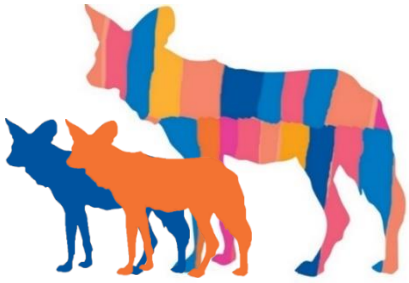
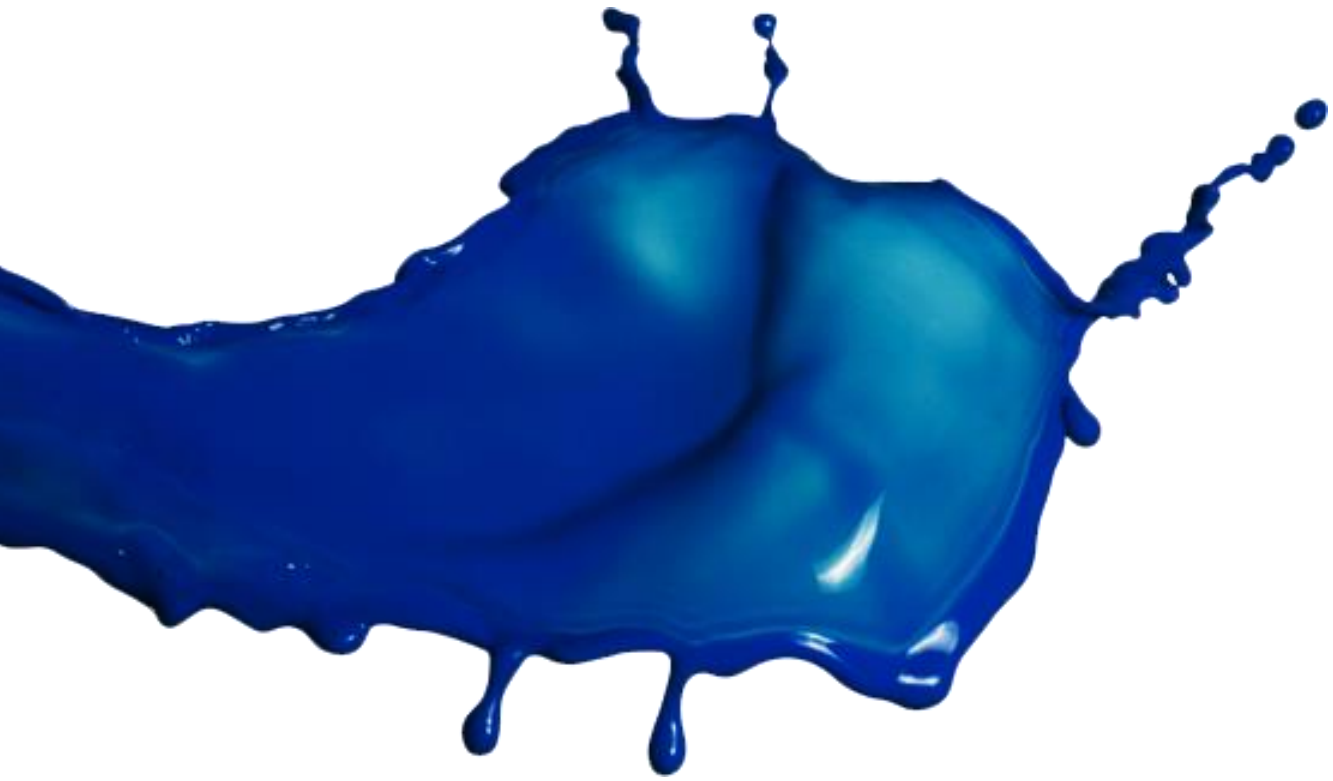
Painted Dog Research

SECURITY INCIDENT RESPONSE PLAN (IRP)

23 September 2019

Contents





Introduction

Introduction

Purpose

This document describes the plan for responding to information security incidents at Painted Dog Research. It defines the roles and responsibilities of participants, characterization of incidents, relationships to other policies and procedures, and reporting requirements. The goal of the Computer Security Incident Response Plan is to detect and react to computer security incidents, determine their scope and risk, respond appropriately to the incident, communicate the results and risk to all stakeholders, and reduce the likelihood of the incident from reoccurring.

Scope

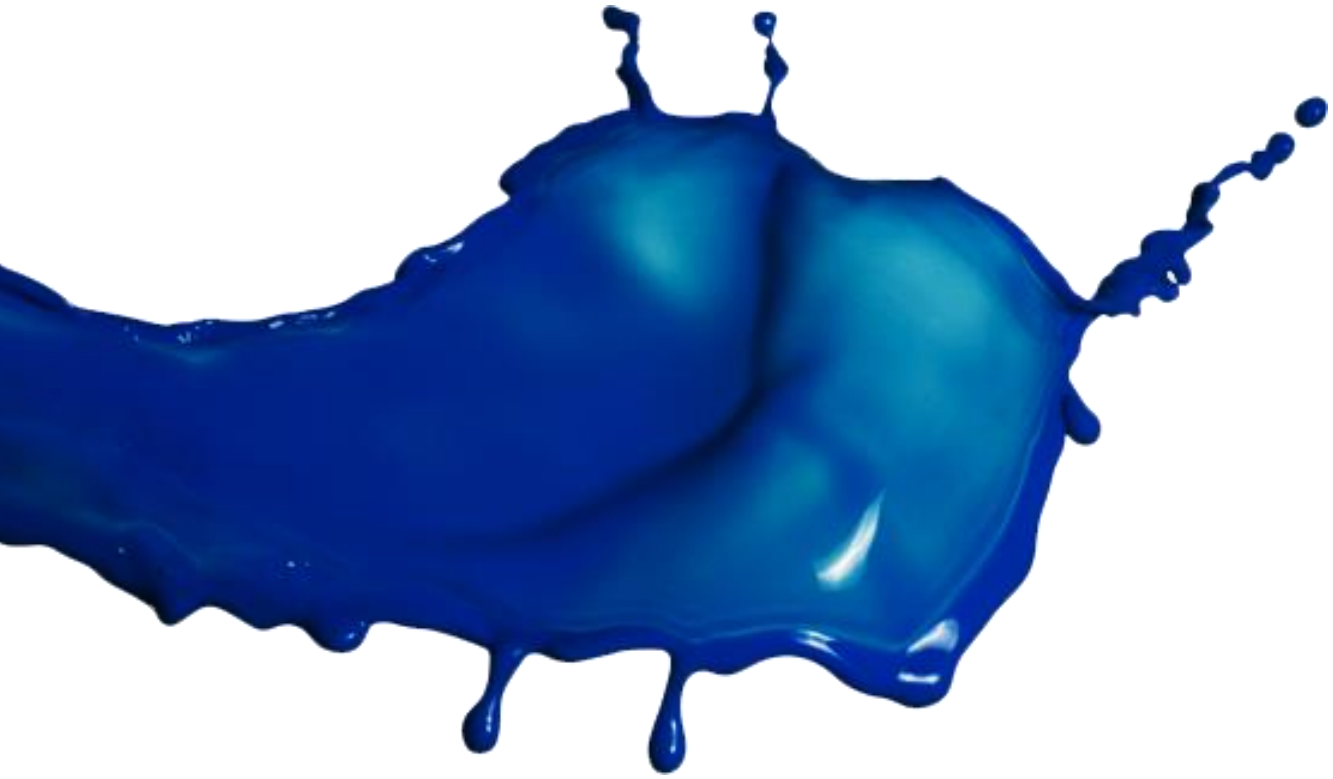
This plan applies to the Information Systems, Data, Information, and Networks of Painted Dog Research and any person or device who gains access to these systems or data.

Maintenance

The Painted Dog Research management team is responsible for the maintenance and revision of this document on annual basis. Our outsourced IT provider is responsible for regularly testing our IRP>

Authority

The PDR Management team is charged with executing this plan by its original charter and various policies such as the Privacy Policy and the IT Compliance Policy.



Definitions

Definitions

Event

An event is an exception to the normal operation of IT infrastructure, systems, or services. Not all events become incidents.

Incident

An incident is an event that, as assessed by PDR management, violates the Computer Use Policy; Information Security Policy, standard, or code of conduct; or Computer Security Incident Response Plan or threatens the confidentiality, integrity, or availability of Information Systems or Institutional Data.

Incidents may be established by review of a variety of sources including, but not limited to PDR monitoring systems, reports from PDR's staff or outside organizations and service degradations or outages. Discovered incidents will be declared and documented in PDR's incident documentation system.

Complete IT service outages may also be caused by security-related incidents, but service outage procedures will be detailed in Business Continuity and/or Disaster Recovery procedures.

Incidents will be categorized according to potential for restricted data exposure or criticality of resource using a High-Medium-Low designation. The initial severity rating may be adjusted during plan execution.

Detected vulnerabilities will not be classified as incidents. PDR employs tools to scan the PDR environment and depending on severity of found vulnerabilities may warn affected users, disconnect affected machines, or apply other mitigations. In the absence of indications of sensitive data exposure, vulnerabilities will be communicated, and PDR will pursue available technology remedies to reduce that risk.

Privacy Identifiable Information

For purpose of meeting security breach notification requirements, Privacy Identifiable Information is defined as:

• Customer data provided by the client that includes the customer's name, contact details, sensitive information, health information, or credit information.

Roles and Responsibilities

The Incident Response Process incorporates the Information Security Roles and Responsibilities definitions and extends or adds the following Roles:

Incident Response Coordinator

The Incident Response Coordinator is a member of an internal management team who is responsible for assembling all the data pertinent to an incident, communicating with appropriate parties, ensuring that the information is complete, and reporting on incident status both during and after the investigation to senior management at PDR with the assistance of external IT security consultants.

Incident Response Handler

Incident Response Handlers are employees of PDR, and external IT consultants who gather, preserve and analyse evidence so that an incident can be concluded.

Insider Threats

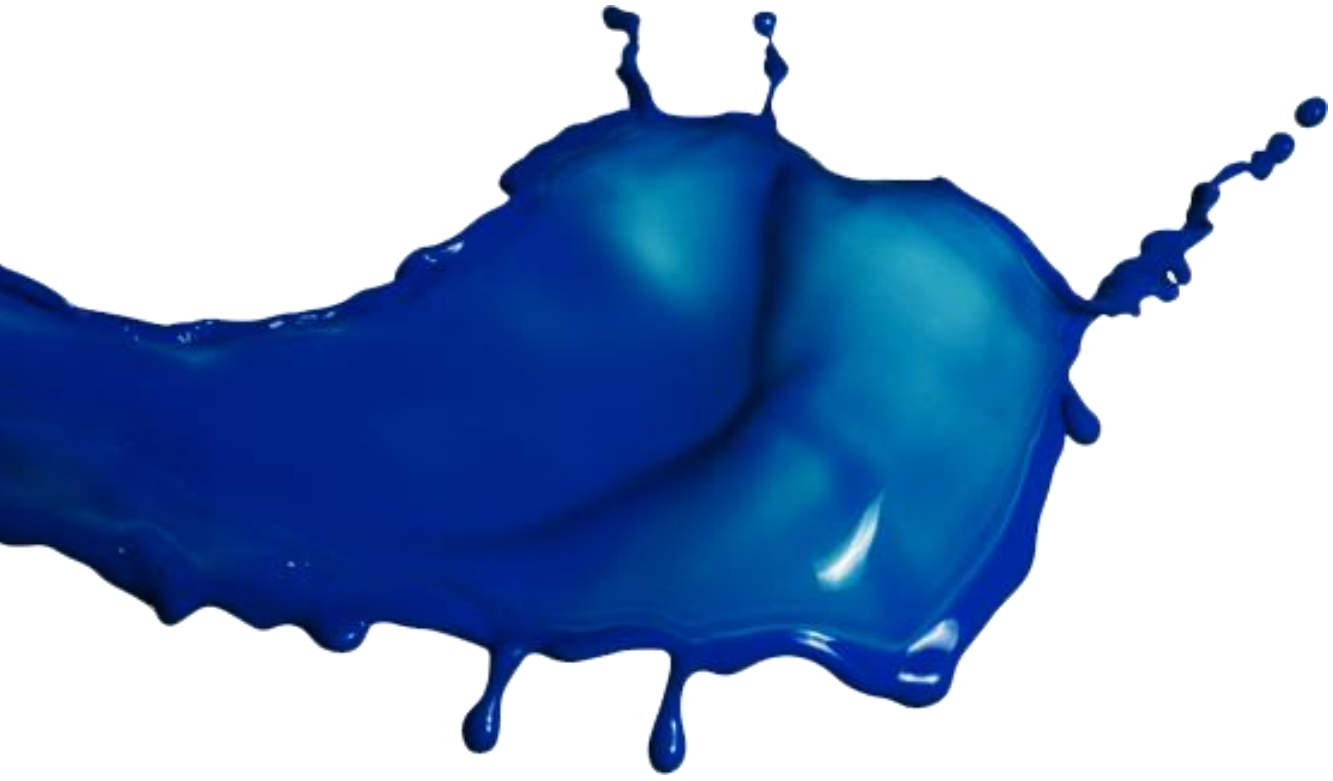
Insiders threats are - current or former employees, contractors, or business partners who have access to an organization's restricted data and may use their access to threaten the confidentiality, integrity or availability of an organization's information or systems. This threat is defined because it requires special organizational and technical amendments to the Incident Response Plan as detailed below.

Law Enforcement

Law Enforcement includes the Western Australian and Federal Police, federal and state law enforcement agencies, and Australian Government agencies that present warrants or subpoenas for the disclosure of information. Interactions with these groups will be coordinated by PDR's senior management team.

Users

Users are PDR staff and consultants or anyone accessing an Information System, Institutional Data or PDR networks who may be affected by an incident



Methodology

Methodology

This plan outlines the most general tasks for Incident Response and will be supplemented by specific internal guidelines and procedures that describe the use of security tools and/or channels of communication. These internal guidelines and procedures are subject to amendment as technology changes. It is assumed that these guidelines will be documented in detail and kept up-to-date.

Support Services

An external IT consulting firm is used to support all Painted Dog Research Information System(s), Data, information, and the userbase. The external IT firm is also responsible for best practice implementation advice in relation to Painted Dog Research security posture, and responds to incidents and threats as part of IT Management service mandate.

Evidence Preservation

The goal of Incident Response is to reduce and contain the scope of an incident and ensure that IT assets are returned to service as quickly as possible. Rapid response is balanced by the requirement to collect and preserve evidence in a manner consistent with the requirements of Australian Privacy Act and Notifiable Data Breaches amendments, and to abide by legal and Administrative requirements for documentation and chain of custody.

Operational-Level Agreements, Governance

Painted Dog Research has operational and management level agreements with third party IT consulting organisations, who provide support and service delivery alongside asset management and systems security monitoring. Painted Dog Research supports the priority of investigation activities in case of incident management and where significant risk exists, accepts responsibility for temporary outages and systems interruptions.

Incidence Response Phases

The basic incident process encompasses six phases: preparation, detection, containment, investigation, remediation and recovery. The overall incident response process includes detection, containment, investigation, remediation and recovery, documented in specific procedures it maintains. This plan is the primary guide to the preparation phase from a governance perspective; local guidelines and procedures will allow Painted Dog Research to be ready to respond to any incident. Recovery includes re-evaluating whether the preparation or specific procedures used in each phase are appropriate and modifying them if inappropriate

1. Preparation

Preparation includes those activities that enable Painted Dog Research to respond to an incident: policies, tools, procedures, effective governance and communication plans. Preparation also implies that the affected groups have instituted the controls necessary to recover and continue operations after an incident is discovered. Post-mortem analyses from prior incidents should form the basis for continuous improvement of this stage.

2. Detection

Detection is the discovery of the event with security tools or notification by an inside or outside party about a suspected incident. This phase includes the declaration and initial classification of the incident.

3. Containment

Containment is the triage phase where the affected host or system is identified, isolated or otherwise mitigated, and when affected parties are notified and investigative status established. This phase includes sub-procedures for seizure and evidence handling, escalation, and communication.

4. Investigation

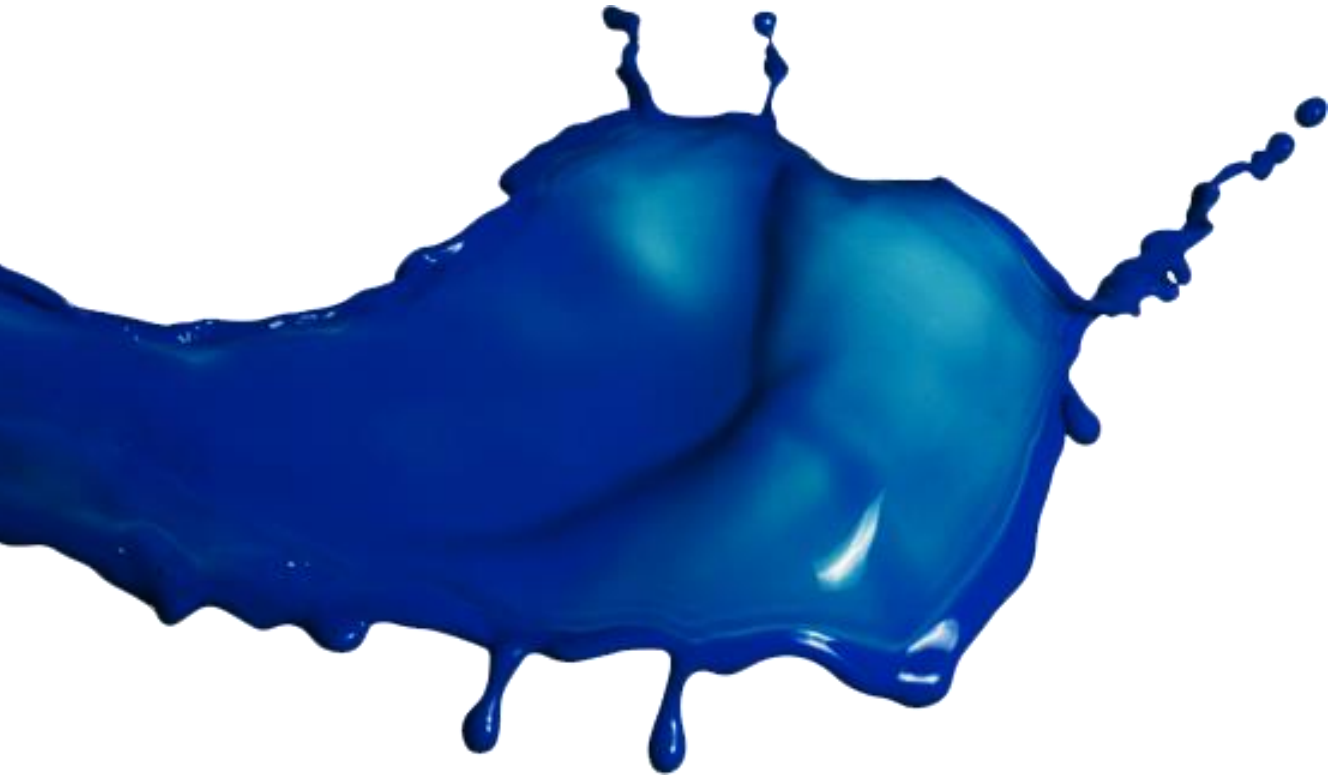
Investigation is the phase where Painted Dog research and external IT personnel determine the priority, scope, and root cause of the incident.

5. Remediation

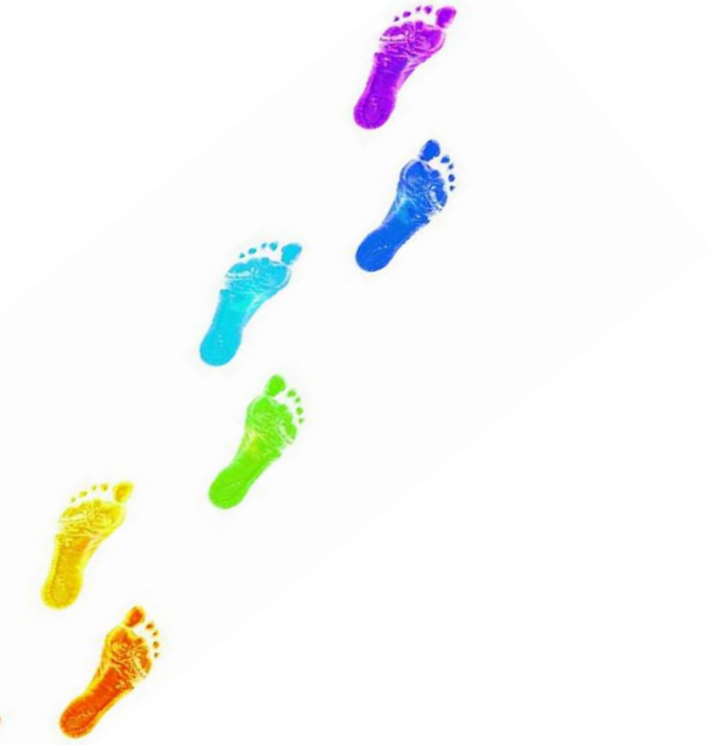
Remediation is the post-incident repair of affected systems, communication and instruction to affected parties, and analysis that confirms the threat has been contained. The determination of whether there are regulatory requirements for reporting the incident (and to which outside parties) will be made at this stage in cooperation with Painted Dog Research management. Apart from any formal reports, the post-mortem will be completed at this stage as it may impact the remediation and interpretation of the incident.

6. Recovery

Recovery is the analysis of the incident for its procedural and policy implications, the gathering of metrics, and the incorporation of “lessons learned” into future response activities and training. Specific procedures related to this Incident response plan are documented at the IT consulting firm Policies and Procedures internal knowledgebase.



Guidelines for the Incident Response Process



Guidelines for the Incident Response Process

In the process of responding to an incident, many questions arise and problems are encountered, any of which may be different for each incident. This section provides guidelines for addressing common issues. The Incident Response Coordinator needs to be consulted for questions and incident types not covered by these guidelines

Insider Threats

In the case that a Incident Response Handler is a person of interest in an incident, the Incident Response Coordinator will assign other Incident Response Handlers to the incident.

Interactions with Law Enforcement

All communications with external law enforcement authorities are made after consulting with senior management at Painted Dog Research.

Communications Plan

All public communications about an incident or incident response to external parties outside of Painted Dog Research are made in consultation with senior management at Painted Dog Research. Private communications with other affected or interested parties contain the minimum information necessary. The minimum information necessary to share for a incident is determined by the Incident Response Coordinator in consultation with Painted Dog Research IT external security consultant.

Privacy

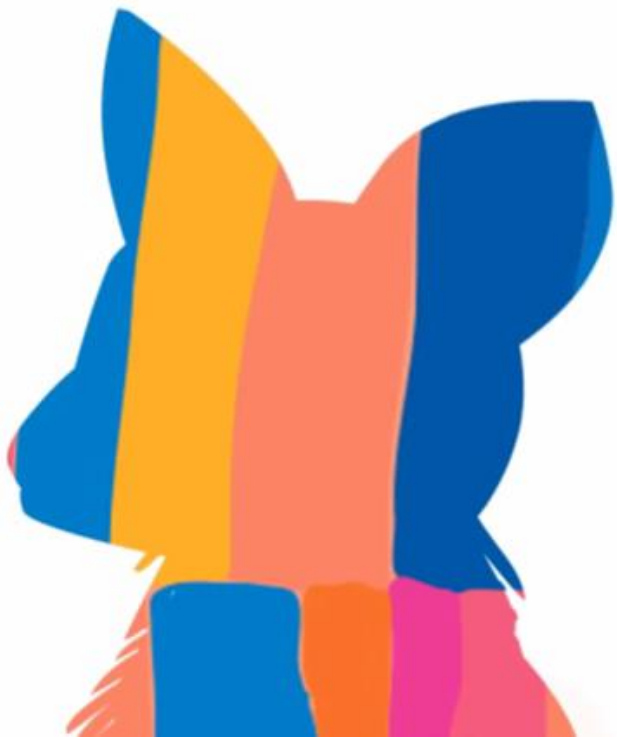
The Privacy Policy provides specific requirements for maintaining the privacy of Painted Dog Research partners and customers. All incident response procedures will follow the current privacy requirements as set out in the Painted Dog Research Privacy Policy. Documentation, Tracking and Reporting All incident response activities will be documented to include artefacts obtained using methods consistent with chain of custody and confidentiality requirements. Incidents will be prioritized and ranked according to their potential to disclose restricted data.

Incidents will be reviewed post-mortem to assess whether the investigational process was successful and effective. Subsequent adjustments may be made to methods and procedures used by the Painted Dog Research and by other participants to improve the incident response process. Artefacts obtained during an investigation may be deleted after the conclusion of the investigation and post-mortem analysis.

Escalation

At any time during the incident response process, the Incident Response Coordinator may be called upon to escalate any issue regarding the process or incident. The Incident Response Coordinator in consultation with Painted Dog research management and IT External consultants will determine if and when an incident should be escalated to external authorities.

Hunt Smarter.



Painted Dog Research Suite 1, Level 2, 658 Newcastle Street Leederville WA 6007
T/F 08 9227 6464 **E** info@painteddogresearch.com **W** painteddogresearch.com