ACC 162A

ACC Confidentiality and Information Security Agreement

"To be completed by the manager who authorises access by Temporary staff, contractors or consultants to the ACC computer and telephone Network"

ACC
PREVENTION. CARE. RECOVERY.
Te Kaporeihana Āwhina Hunga Whara

Temporary staff/Contractor/Consultant details

(You must complete this form by the end of your first day of network access)

Name: Simon Howard Position/WR No ....

Employment Status: (circle) Temporary staff [✓ Consultant] Contractor

Terms and Conditions

(You must read the following prior to signing)

I have read the requirements detailed on this form and I understand and agree to comply with them, during my employment and after my employment ceases with ACC. I understand that if I fail to sign or comply with this agreement it may result in termination of my and/or my employer's contract with ACC in accordance with ACC's policies and procedures.

Agreement

I agree to uphold and follow the Information Security policies and standards which my ACC manager will arrange to show and explain to me. In addition to the compliance with policies and standards, I agree that:

1. I will be responsible for any access made by me on any ACC computer system, network, application or database.
2. I will not give my password(s) to anyone else and will not use another person's user identity or password.
3. I will log my computer off at the end of each working day, unless I have permission from my manager to run an overnight batch job or for some other authorised reason.
4. I will not remove any computer hardware (including components of hardware, USB devices), software, publications, drawings, or other information or asset from ACC offices without my manager's authority.
5. I will not incorporate, install or connect, hardware (including, but not limited to, laptops, USB devices, modems) or software onto an ACC workstation (includes laptops) or server without first obtaining approval from ACC's BT staff through formal processes. For developers, approval must be gained from the Project Manager who will ask BT staff for approval, through Change Delivery management.
6. When I leave ACC employment, I will return to ACC all documentation and property belonging to ACC or its associates, subsidiaries, agents, suppliers, customers or claimants provided or gained by me in the course of my work at ACC or for its subsidiaries or business partners.
7. I will not access information beyond my level of delegation or authority, nor will I access information for others who are not entitled to view that information.
8. I will not allow another person to use my security access card/key/code to give access to any ACC information, systems or documentation.
9. I will not reveal any non-public information that comes to me in the course of my employment at ACC including but not limited to, personal information about employees, levy payers, claimants, service providers, policy holders, advisors or any other stakeholder, regardless of how that information came to my knowledge. This clause does not apply to information required by an authorised officer of ACC, other authorised persons, or information required by compulsion of law.

Other relevant ACC Policies

Asset Management Policy – ACC assets must not be used for personal use without prior approval from the appropriate Cost Centre manager.

Unauthorised use of Information - the unauthorised 'giving away' or selling of ACC held information or material by an employee, acting on their own behalf, is legally termed theft. Any such instance may result in instant suspension or termination of contract. ACC, at its discretion, may inform the Police of such activity.

User signature:		Date:	8/1/2014		
Authorising Manager's Name:		Date:		Signature:	

The authorising signatory must ensure that the temporary staff member, new contractor or consultant is given induction training on information security as stated in this agreement; it may also help to pass them a copy of the 'Quick Guide' to Information Security.

The authorising signatory or delegated manager must hold a completed copy of this form for inspection by internal audit.

PREVENTION. CARE. RECOVERY.

12/19/2013

Open Source Intelligence Training

Statement of Work

Version: 1.2

Table of Contents

1 Document Control

1.1 Document Information

Customer	ACC
Title	Open Source Intelligence Training - Statement of Work
Document Filename	ACC - OSINT Training SoW v1.2

1.2 Revision Control

Version	Date Released	Pages Affected	Author	Description
0.1	11/12/2013	All	Simon Howard	Initial Draft
1.0	15/12/2013	All	Simon Howard	Release for comment
1.1	17/12/2013	All	Simon Howard	Incorporate feedback
1.2	19/12/2013	All	Simon Howard	Final Release

1.3 Distribution List

Name	Organisation	Title
9(2)(a)	Accident Compensation Corporation	National Manager Investigations
Simon Howard	ZX Security Limited	Security Consultant

2 Background

Simon Howard met with 9(2)(a) from the Accident Compensation Corporation (ACC) to discuss the delivery of training material to his investigative staff.

The ACC investigative unit deals with around 1400 cases of fraud against ACC a year. The perpetrators of the fraud often leave evidence of their actions online where an investigator can collate it to assist them in putting together a case.

In order to assist his staff in performing their duties more efficiently, 9(2)(a) has requested that training material be developed to cover tools and techniques used for gathering information from open-source and social media sources.

This statement of work details the tasks that will be conducted as part of the OSINT training, the associated costs and estimated timeframes.

3 Objectives

The objective of this engagement is to:

- Increase the knowledge of the ACC investigation team regarding Open-Source Intelligence (OSINT) and Social Media Intelligence (SOCMINT)
- Introduce team members to the latest tools and techniques used to extract data from OSINT/SOCMINT sources to support their day-to-day work activities

4 Scope

The scope of this engagement is as follows:

- Delivery of one unique day-long OSINT course to ACC employees

5 Approach

The approach used to deliver this presentation will be as follows:

- Research topics and prepare slide deck material
- Prepare workshop material including software and module tasks
- Prepare virtual machines as a takeaway from the course for installation on the attendees home computers
- Deliver course material to ACC employees

6 Deliverables

The following deliverable will be produced as part of this statement of work

- A day-long course on open-source intelligence gathering techniques delivered as a PowerPoint presentation and a series of modules.
- The course will run from 09:00 to 17:00

The course will be run as a series of modules which each module discussing one or more topics. Each topic will involve hands-on exercises involving the course attendees where they will gain real-world experience with the tools and techniques discussed.

Module	Topic	Description	Duration (mins)
Operational Security - Introduction			
	OPSEC practices	An overview of operational security processes and measures	30
Internet Fundamentals			
	Internet fundamentals (DNS, SMTP, TCP/IP)	An overview of the building blocks of the Internet, description of how IP Addresses, DNS and SMTP work at a basic level	45
Operational Security – Remaining Undetected			
	Methods for masking your IP address	Details of the various methods that can be used to mask your IP address including TOR, VPNs' and Jump-hosts	30
	Virtualisation as a tool to avoid being compromised	Walk through the virtual machine environment which will be provided to each attendee and explanation of how the technology works	30
Open Source Intelligence Gathering			
	OSINT/SOCMINT information sources	Details of the open-source and social media sources that can be used to build a profile on an individual	25
	Using search engines like a pro	Using search engines to find exactly what you are looking for by becoming a google power user	20
	Tools and techniques used for information gathering	A run through the tools (open-source and commercial) used for information gathering and analysis	80
	Image metadata analysis	Details on how to extract meta-data from images including GPS coordinates and device information (e.g. mobile phone/camera model)	30

	Monitoring chat channels and forums	How to connect to and monitor chat rooms and forums (both on the Internet and the Deep Web)	80
Maintaining multiple covert identities			
	Detecting fake profiles	Techniques used to identify a fake profile. .	10
	Cross-posting & profile management	How to maintain multiple identities across various social networks	20
	Profile backstopping	Techniques for creating a backstop (history) for your online personas	20
	Anonymous cell phone numbers and email addresses	Systems and processes for sending and receiving anonymous messages (SMS and Email).	20
	Payment methods for purchasing services	How to pay for various services while maintain anonymity	10
Workshop			
	Creating a Dossier	During this workshop the attendees will use the skills gained during the course to create a detailed dossier on a particular individual	30

7 Project Structure

This project will be resourced as follows:

Role	**Name**	**Organisation**
Security Consultant	Simon Howard	ZX Security Limited

8 Assumptions

The following assumptions have been made:

- ZX Security will provide a location to hold the training course which has the necessary seating to accommodate the numbers and a projector to display the training material
- ZX Security will provide each course attendee with a computer to run the workshops on
- The course will be delivered to staff in Wellington
- All work will be conducted during normal business hours

9 Project Schedule

Based on the scope of work as outlined above we have scheduled two sessions, each will deliver the same course material on the following dates:

- 19th and 20th February 2014

10 Project Costs

The assignment has been priced on a time and materials basis for the course material preparation and a fixed-price for delivery of the course material.

Stage	Number	Hours	Rate	Total
Course Material Preparation		16	$200	$3,200.00
Course Delivery (2 days)	2		$1,600	$3,200.00
Training Room Hire (2 days)	2		$990	$1,980.00
Total				$8,380.00

If ACC wish to deliver this course again at any stage, it will be charged at ZX Security's standard daily rate of $1600/day. If a training room and computers for attendees are also required then additional costs will be incurred.

All quotes exclude GST and disbursements. Should the project scope change, we will work with the ACC project manager to ensure an appropriate resolution can be reached.

11 Acceptance

The project as defined within this document is deemed acceptable, and gives approval to proceed with the assignment as described.

9(2)(a)

20/12/13

9(2)(a) - ACC

Date

Simon Howard 8/1/2014

memorandum

PREVENTION. CARE. RECOVERY.
Te Kaporeihana Āwhina Hunga Whara

To	***All Course Attendees*** ***Investigation Managers***
From	9(2)(a)
Date	***14 January 2014***
Subject	***General Instruction - Open Source Intelligence Course***

Introduction

In the 21st century, technology is a significant influence on the way society and business is structured, and is a driver for both social and business evolution. Business processes today are fundamentally different from what they were a decade ago and consequently the methods and techniques by which groups and individuals may wish to exploit and create harm to an organisation such as ACC, have changed.

The internet now enables significant business interaction between organisation and the client, business to business remote transactions, information sharing, social interaction and communication.

These changes pose both a risk and opportunity for our counter fraud function of protecting ACC's reputation and loss through fraud. The risk posed by e-business fraud and multiple identities is an emerging business risk that can be addressed by appropriate business design and prevention disciplines. The opportunity presented by undisciplined, open, online social communication assists in the determination of intent and identification of individuals or entities that wish to harm ACC. This opportunity presents ACC with a tool to detect and defeat the fraudster's intent.

Training Outcome

This course is designed to be both theoretical and practical and to introduce participants, at a basic level, to open source information in the cyber environment. It will enable interaction with sources and provide tools for this interaction. A detailed syllabus is attached.

Open Source Intelligence

Open source intelligence or "OSINT" refers to an information gathering discipline based on the collection and analysis of information from open sources, i.e. information available to the general public. These sources include newspapers, the internet, books, telephone books, scientific journals, sporting and recreation associations, credit information and others.

Course Dates

The course will be run for two groups of eight participants on 19 and 20 February 2014. Each course is one day's duration. Participants have been advised of their acceptance and the date of their course.

The Instructor

The course content will be delivered by IT Security Consultant, Simon Howard from ZX Security Limited.

Simon has worked in the IT Security industry for the past 13 years and over this time has undertaken a number of different roles ranging from Security Engineer (Building systems), to Penetration Tester (Breaking into systems) to Security Consultant (Helping people fix their systems).

Simon has presented research on security issues across the globe, his research into defeating antivirus products garnered international press attention and was covered by the likes of Forbes magazine.

During his spare time Simon helps run Australasia's largest information security (hacking) conference, Kiwicon which is in its 8th season and last year was attended by 800 security enthusiasts.

Training Location

The course will be conducted at:

Auldhouse
Level 8,
Lumley House,
11 Hunter Street
Wellington

The course will commence at 9.00 am and will finish at 5.00pm.

A lunch voucher will be supplied to each participant ~~for~~ to the value of $12 that can be used at 20 different food outlets in the area. ~~Normal t~~Tea and coffee facilities will be available in the training room.

Travel

As advised on 19 December 2013 participants cost centres are responsible for all travel.

I trust you fine the training professionally challenging, rewarding and enjoyable.

9(2)(a)
National Manager Investigations

Attachment 1. Detailed syllabus

Attachment 1. Detailed syllabus

The course will have a series of modules with each module discussing one or more topics. Each topic will involve a hands-on exercise involving the attendees where you will gain real-world experience with the tools and techniques discussed.

Module and Topic	Description
Operational Security – Introduction	
OPSEC Practices	An overview of operational security processes and measurements
Internet Fundamentals	
Internet fundamentals (DNS, SMTP, TCP/IP)	An overview of the building blocks of the Internet, description of how IP Addresses, DNS and SMTP work at a basic level
Operation Security – Remaining Undetected	
Methods for Masking your IP address	Details of the various methods that can be used to mask your IP address including TOR, VPNs' and Jump-hosts
Virtualisation as a tool to avoid being compromised	Walk through the virtual machine environment which will be provided to each attendee and explanation of how the technology works
Open Source Intelligence Gathering	
OSINT/SOCMINT information sources	Details of the open-source and social media sources that can be used to build a profile on an individual.
Using search engines like a pro~~Using Google like a pro~~	Using search engines to find exactly what you are looking for by becoming a google power user~~Using Google to find exactly what you are looking for by becoming a Google power user.~~
Tools and techniques used for information gathering	A run through the tools (open-source and commercial) used for information gathering and analysis.
Image metadata analysis	Details on how to extract meta-data from images including GPS coordinates and device information (e.g. mobile phone/camera model).
Chat channels and forums	How to connect to and monitor chat rooms and forums (both on the Internet and the Deep Web).
Maintaining multiple identities	
Detecting fake profiles	Techniques used to identify fake profiles.
Cross-posting and profile management	How to maintain multiple identities across various social networks.
Profile backstopping	Techniques for creating a backstop (history) for your online personas.
Anonymous cell phone numbers and email addresses	Systems and processes for receiving anonymous messages (SMS and Email).
Payment for purchasing services	How to pay for various services while maintaining anonymity
Workshop	
Creating a Dossier	During this workshop the attendees will use the skills gained during the course to create a detailed dossier on a particular individual

ZX SECURITY

TAX INVOICE

GST Number: 112-947-337
INVOICE #2014030600
DATE: MARCH 6, 2014

Simon Howard
5 Karepa St
Brookyln
Wellington 6021
New Zealand
accounts@zxsecurity.co.nz
+64 9(2)(a)

BILL TO:
Attn: 9(2)(a)
Accident Compensation Corporation (ACC)
Justice Centre
19 Aitken Street
PO Box 242
Wellington 6140

DESCRIPTION	PROJECT CODE	UNITS	UNIT PRICE	TOTAL
Course Material Preparation		16	$200.00	$3,200.00
Course Delivery (2 days)		2	$1,600.00	$3,200.00
Training Room Hire (2 days)		2	$990.00	$1,980.00
			SUBTOTAL	$8,380.00
			G.S.T	$1,257.00
			TOTAL DUE	$9,637.00

This invoice is payable to ZX Security Limited
BNZ Bank Account Number: 9(2)(a)

If you have any questions concerning this invoice, contact Simon Howard on 9(2)(a)

9(2)(a)
National Manager Investigations