



Our ref PN00004

Advanced Personnel Management  
Unit 4, Level 1, 35 Gordon Ave  
GEEELONG WEST VIC 3218

Dear

**jobactive Deed 2015-2020  
Breach of Privacy**

I refer to the jobactive Deed 2015-2020 ('the Deed') between Serendipity (WA) Pty Ltd (ABN 64 062 160 614) ('Your Organisation') and the Commonwealth, as represented by the Department of Employment ('the Department'). I am writing to you regarding a breach of the *Privacy Act 1988 (Cth)* ('the Privacy Act') and section 4.1 of the Records Management Instructions (RMIs).

I refer to your initial email of 1 October 2015 alerting the Department to the incident that occurred on 30 September 2015. You advised that devices and Records containing the personal information of a number of job seekers were stolen from the vehicle of [REDACTED] an employment consultant at Your Organisation.

*Data breach under the Privacy Act*

As a contracted service provider, clause 35 of the Deed provides that Your Organisation must not act in a way that would breach the Department's privacy obligations if done by the Department itself. The sources of these obligations include the Privacy Act and the Office of the Australian Information Commissioner's Guide, 'Data breach notification – A guide to handling personal information security breaches' ('the Guide').

In assessing whether the circumstances resulted in a data breach, the Department has referred to the Privacy Act and the Guide. The Guide provides that a data breach occurs when personal information is 'lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference'. The Department is satisfied that a data breach has occurred because of the loss of personal information from this incident.

The Guide contains information on how Your Organisation may choose to respond to a data breach and the factors that you should consider in framing such a response. The Guide suggests that if a data breach is identified, a decision on how to respond should be made on a case by case basis, considering the personal information involved, the extent that information was disclosed, the cause and extent of the breach and the risk of harm. In some circumstances, it may be appropriate to notify affected individuals or the Office of the Australian Information Commissioner (OAIC) of the data breach.

In these circumstances, the Department considers that it is not necessary for Your Organisation to inform the affected individuals or the OAIC of the data breach. However, this is a matter that Your Organisation should consider for itself, having regard to the Guide.

### *Breach of RMIs - unauthorised removal of Records*

In addition to the data breach, Your Organisation has breached section 4.1 of the RMIs. Section 4.1 relevantly states 'Providers must ensure Records are protected from... unauthorised alteration or removal'. The RMIs form a Guideline for the purposes of the Deed.

Your Organisation breached section 4.1 because it did not ensure protection of the Records from unauthorised removal. The removal of Records was clearly not authorised by Your Organisation or the Department.

### *Your Organisation's response to breaches*

On 12 October 2015, the National Office wrote to your Account Manager requesting further information regarding the breach which was provided by your office on 6 November 2015.

The Department is satisfied that all staff in Your Organisation have been advised of the correct procedures to adopt when attending Outreach sites and has emphasised that when travelling to Outreach locations, storage of any of Your Organisation's equipment or materials should be in the boot of the vehicle. The Department is satisfied with the 'all staff' communication to all employment services staff regarding their responsibilities concerning jobseeker privacy and Your Organisation's obligations with respect to data.

The Department sought assurances from Your Organisation that it has appropriate processes and procedures in place to protect the personal information. The Department acknowledges that Your Organisation has a comprehensive Privacy Policy and provides training to its staff members including ensuring each staff member sign an acknowledgement that they understand 'acceptable use' of computing equipment. We therefore do not believe this is a systemic issue, rather a failure to follow a policy by an inexperienced staff member.

### *The Department's actions in response to breaches*

Based upon the action taken by Your Organisation since becoming aware of the breach, the Department is of the view that Your Organisation has undertaken appropriate and reasonable steps to resolve this matter. The Department will record the incident as a low impact breach against Your Organisation. In this case, the Department does not propose to take action in relation to the breach.

Please be aware that any future instances of non-compliance by Your Organisation may be considered along with the issues detailed in this letter, and the Department may take action in respect of Your Organisation's aggregate non-compliance.

The Department takes matters of non-compliance very seriously and I remind you that such matters can be taken into account when considering future performance and business reviews. I urge Your Organisation to maintain a strong focus on robust administration and governance. I also encourage Your Organisation to be attentive to all programme assurance review feedback supplied by the Department.

If you wish to discuss this matter or require further information, please contact your Account Manager, on 03 5430 5629.

Yours sincerely

Branch Manager  
Providers and Purchasing Branch  
Department of Employment

14 June 2016



Our ref PN00005

Western District Employment Access Inc.  
52 Fairy Street  
WARRNAMBOOL VIC 3280

Dear

**jobactive Deed 2015-2020  
Breach of Confidentiality**

I refer to the jobactive Deed 2015-20 ('the Deed') between Western District Employment Access Inc. (ABN 18 781 854 750) ('Your Organisation') and the Commonwealth, as represented by the Department of Employment ('the Department'). I am writing to you regarding a breach by Your Organisation of the Records Management Instructions (RMIs).

The RMIs form a Guideline for the purposes of the Deed. Section 4.1 of the Record Management Instructions (RMIs) relevantly states that 'Providers must ensure Records are protected from ...unauthorised alteration or removal'.

Your Organisation's initial email of 8 October 2015 alerted the Department to a confidentiality breach that occurred on 5 October 2015. Your Organisation stated that a former employee, while still employed at Your Organisation sent an attachment containing details of her jobactive caseload involving 117 clients to her personal email address.

Your Organisation breached Section 4.1 of the RMIs by not ensuring protection of the clients' details from unauthorised removal. removal of the Records was clearly unauthorised by either the Department or Your Organisation.

The Account Manager requested further information regarding the breach which Your Organisation provided on 11 November 2015. The Department acknowledges that Your Organisation engaged a solicitor on this matter. The solicitor provided advice that as an ex-employee was bound to abide by the contractual duty of confidentiality as an employee. The solicitor wrote to on two separate occasions, initially requesting she sign a statutory declaration; and secondly advising Your Organisation was entitled to commence legal proceedings to issue an injunction which would require her to abide by the duty of confidentiality.

The Department acknowledges: failed to respond on both occasions. Your solicitor advised that the costs associated with bringing the court action would be significant and may not be justifiable.

The Department is satisfied that Your Organisation has undertaken appropriate and reasonable steps to resolve this matter. The Department will record the incident as a low impact breach against Your Organisation. In this case, the Department does not propose to take action in relation to the breach.

Please be aware that any future instances of non-compliance by Your Organisation may be considered along with the issues detailed in this letter, and the Department may take action in respect of Your Organisation's aggregate non-compliance.

The Department takes matters of non-compliance very seriously and I remind you that such matters can be taken into account when considering future performance and business reviews. I urge Your Organisation to maintain a strong focus on robust administration and governance.

If you wish to discuss this matter or require further information, please contact your Account Manager, on 03 5430 5629.

Yours sincerely

Branch Manager  
Providers and Purchasing Branch  
Department of Employment

14 June 2016



Australian Government  
Department of Employment

National Office

Your Ref  
Our Ref: ES-15-11042

Sarina Russo Job Access (Australia) Pty Ltd (SRJA)  
Level 6  
Sarina Russo River Plaza  
100 Eagle Street  
Brisbane City QLD 4000

Dear

**jobactive Deed 2015-2020 – Records related incident**

I am writing to you regarding the incident involving the security and management of job seeker records at your (former) Narre Warren site in Victoria. The department was notified about the incident by the Office of the Member of Parliament for Holt.

The department acknowledges your organisation's action in reporting the incident to the Office of the Information Commission on the 27 May 2016 and your efforts in keeping us informed of your progress during your investigation of the incident.

On 5 July 2016 you provided the department with a detailed response of your investigation and findings, including the extent and content of the records involved and the events leading up to the incident. Your report of the incident confirms that in the course of relocating your offices at Narre Warren, the relevant clauses of the Deed and other legislation, as outlined in Attachment A, including internal records management processes were not fully complied with and you concluded that carelessness and human error contributed to the incident, rather than systemic processes for the overall management of records.

The department considers that the removal of the secure destruction bin on 20 May 2016, one week before the final vacation of the premises at Narre Warren also contributed to the inappropriate disposal of documentation by your staff.

jobactive providers must comply with all of their obligations under the Deed, including compliance with privacy and other legislation. The department treats any failures to comply with these requirements very seriously, regardless of how it occurs, and it is important that

rectification action is taken, as soon as possible, to prevent incidents of this nature reoccurring in the future.

The department notes and agrees with the steps that your organisation intends to take following the incident, to reduce the risks and prevent further incidents.

Accordingly, I seek your reassurance and agreement to the following actions outlined in your 5 July 2016 report:

- Update the processes for office relocations including:
  - clearer identification of a single responsible person for managing the process;
  - a revised relocation plan that includes at a minimum, assigned roles, inventory, timeline for the move, resources (e.g. additional Secure Document Destruction bins) and reconciliation process;
  - specific actions associated with compliance with the Records Management Instructions issued to you by us;
  - contingency arrangements for resourcing to ensure sufficient staff resources to achieve the above with caseload management factored into the move; and
  - refresher Privacy and Records Management face to face training will be delivered for all Narre Warren site staff.
- Conduct a review of existing procedures to ensure they comply with your obligations under the Deed regarding records management and privacy to ensure the issues identified in this incident are appropriately covered.

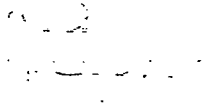
I require you to confirm in writing within fourteen days of the date of this letter your agreement to complete these rectification actions by 10 December 2016. You will also need to report to your Account Manager, that the steps have been taken by 10 December 2016.

The department reserves the right to take further action it deems necessary under the Deed in relation to this privacy breach. Failure to provide updates by the timelines and/or demonstrated compliance with the actions you have proposed will result in a review of this matter and may lead to further actions by the department.

The department does not, at this stage, require your organisation to contact the job seekers whose records were breached by this incident. However, if in the future, job seekers contact the department regarding this incident, the department will reconsider this position.

If you have any questions regarding the details of this letter, please contact \_\_\_\_\_ on (07) 3223 1858 or myself on (02) 6121 6667.

Yours sincerely



Quality and Integrity Group  
10 August 2016

---



## Attachment A

### Deed clauses and legislation non compliance

Specifically, the Department notes that as a result of this incident your organisation has failed to comply with:

- the *Privacy Act 1988 (Cth)* ('the Privacy Act') specifically Australian Privacy Principle (APP) 11 and possibly APP6;
- clause 35.2 of the jobactive Deed in that it failed to comply with the Privacy Act and the APPs as if it were an agency;
- clause 35.4 of the jobactive Deed in that it failed to comply with the requirements under Division 3 [Confidentiality] of Part 5 of the Administration Act when handling Protected Information;
- clause 37.5, 37.7 and 37.11(a) of the jobactive Deed in that it failed to store, control access to and dispose of Records in accordance with the requirements of clause 37;
- clause 93.3 of the Employment Services Deed in that it failed to comply with the Privacy Act and the APPs as if it were an agency;
- clause 93.5 of the Employment Services Deed in that it failed to comply with the requirements under Division 3 [Confidentiality] of Part 5 of the Administration Act when handling Protected Information; and
- clause 96.4, 96.6 and 93.10(a) of the Employment Services Deed in that it failed to store, control access to and dispose of Records in accordance with the requirements of clause 96.

# Sarina Russo Job Access

BRISBANE, SYDNEY, CANBERRA,  
MELBOURNE, ADELAIDE, PERTH  
WEST MIDLANDS, LONDON

HEAD OFFICE • QUEENSLAND  
Sarina Russo River Centre  
Level 6/100 Eagle Street  
GPO Box 856, Brisbane  
Queensland, 4000 Australia

P 13 15 59

f /sarinarussjobaccess  
t @srjobaccess

ABN 21 090 052 350

Your reference: ES-15-11042

18 August 2016

Account Manager  
Queensland State Office  
Department of Employment  
GPO Box 9880  
Brisbane QLD 4001

Cc: [REDACTED]

Quality and Integrity Group  
Department of Employment

Dear

Re: jobactive Deed 2015-2020 – Records related incident

I refer to the correspondence from [REDACTED], Quality and Integrity Group, dated 10 August 2016 in relation to the incident at the former Sarina Russo Job Access (SRJA) Narre Warren site regarding participant records. We appreciate the Department's comprehensive response and note the Department's agreement to the steps taken by SRJA following the incident to reduce the risks and prevent further incidents.

[REDACTED] required in writing within 14 days our agreement to complete rectification actions outlined in her correspondence by 10 December 2016.

We confirm our agreement and provide the following update:

#### Processes for office relocations

- a) [REDACTED] SRJA, as the contract owner, is ultimately responsible for any site relocations. The [REDACTED] appoints an appropriate senior executive to be the single point responsible for project management oversight of site relocations, working hand-in-hand with the SRJA Property Team which is comprised of the SRJA National Property Manager and the in-house property team.



**jobactive**  
an Australian  
Government Initiative

**Sarina Russo**  
Energising People.  
Enhancing Lives

sarinarusso.com

Since 1979

 Disability  
Employment  
Services  
AN AUSTRALIAN GOVERNMENT INITIATIVE

- b) A revised relocation plan – the updated *SRG Office Relocation Process* is at Attachment A.
- c) The *SRG Office Relocation Process* contains specific actions (associated with the requirements for transfer, storage and destruction of documents which contain personal information) to ensure compliance with the Deed and Records Management Instructions. Refer to section 4.7 of the *SRG Office Relocation Process*.
- d) Contingency arrangements for resourcing – The relevant SRJA state manager and/or regional manager directly monitors the progress of the site that is relocating and identifies if additional staff or infrastructure resources are required. The nominated project manager for the relocation is authorised to deploy additional resources to ensure the integrity of the move. SRJA Head Office staff (and staff from other SRJA jobactive or DES site/s) will assist with the site relocation, to allow the site staff to continue to manage their caseload in line with jobactive servicing requirements.
- e) Refresher privacy and records management face to face training to Narre Warren site staff – targeted privacy and records management training was delivered on 20 July 2016 by [redacted] site staff at the Narre Warren site.
- f) The SRJA CEO is writing to individual staff operating from the Narre Warren site outlining their responsibilities in respect of privacy and records management. All staff must confirm in writing they understand their responsibilities and obligations, and will adhere to the documented privacy policy and protocols along with the relevant contractual requirements.

SRJA is relocating its Helensvale jobactive site in September 2016 and will follow the revised office relocation process.

#### Review of existing procedures

As identified under "ongoing and continuing actions" in our Report on the Narre Warren data incident and consistent with good quality management practice, we continue to review our existing procedures. For example, we have implemented tighter processes for site relocations:

- a) An immediate report following the conclusion of a site relocation and cessation of the lease will be provided by the project manager to: the SRJA [redacted]; the SRJA [redacted]; and the SRJA [redacted].
- b) Outcomes of site relocations will be reported to the SRJA Risk Management and Compliance Committee as part of the Legal and Property Report (standing agenda item).
- c) [redacted] Sarina Russo White House (SRJA's in-house cleaning company) will coordinate the end-of-lease cleaning of the premises in the weeks prior to the relocation to ensure particular vigilance and adherence to our instructions regarding records management and document destruction.
- d) In addition to the existing [redacted] secure document destruction bin(s) at the site, extra secure document destruction bin(s) or similar secure receptacles will be deployed in the period leading to the relocation.

SRJA governance forums for June and July 2016 have included specific focus on records management and privacy obligations under the various deed and related guidelines. For example:

- a) The June and July Executive Operations meetings discussed privacy and records management and our obligations under the RMIs and Deeds.
- b) The Risk Management and Compliance Committee meetings included privacy and records management as a standing item.
- c) Site managers conducted sessions with their site staff to reinforce the records management and privacy obligations.

SRJA will review other procedures to ensure they comply with our obligations under the Deed. SRJA is working towards the Department's deadline of 10 December 2016.

SRJA takes its privacy and records management obligations under the Deed seriously and is committed to continuously improving its records management and site relocation process.

I trust this addresses the Narre Warren matter. I look forward to meeting with you on 6 September 2016 for our Performance Period 2 discussion.

Yours sincerely

Sarina Russo Job Access

---



Australian Government  
Department of Employment

Your Ref  
Our Ref ESFS-288244

MAX Employment  
Building 4/107 Miles Platting Road  
EIGHT MILE PLAINS QLD 4113

Dear

**Suspected Unauthorised Access to Departmental Systems —**

I refer to our letter to you of 19 August 2016 in relation to the department undertaking an investigation into the suspected unauthorised access to the department's IT system (ESS) by staff members of your subcontractor Sureway Employment and Training Pty Ltd, namely [REDACTED]. I am now writing to advise that the investigation into the alleged unauthorised access to ESS by [REDACTED] has been completed.

Based on the department's investigation, we conclude that [REDACTED]'s access to ESS on 3 May 2016 was appropriate and authorised. However, the department considers that [REDACTED]'s access to ESS on 12 and 24 February 2016 which was unauthorised and improper as she accessed job seeker records for personal reasons. I note that [REDACTED] is working exclusively on the MAX Employment subcontract, and therefore this matter falls under your organisation's responsibility.

Clause 32.14 of the jobactive Deed (Deed) provides that the Provider must ensure that its Subcontractors comply with the Department's Security Policies. The Department's Security Policies provide that:

*All use of the Department System must be for authorised purposes. Use of facilities for any unauthorised purpose ... is improper use of the facilities and a breach of this Policy.<sup>1</sup>*

*A breach of this Policy occurs when any person performs an act prohibited by the Policy. Examples include: ...*

- users using the system for a purpose not authorised by the Department<sup>2</sup>*

<sup>1</sup> Security Policy for External Service Providers and Users, section 3.6.1

<sup>2</sup> Ibid, section 3.7

2.

The investigation found that the unauthorised access to ESS by [redacted] was an improper use of the facilities. Accordingly, your organisation has failed to ensure that its subcontractors comply with the Department's Security Policies and is in breach of clause 32.14 of the Deed.

Given the seriousness with which the department views security and privacy, and pursuant to clause 32.18(a) of the Deed, the department has taken action to terminate [redacted] access to ESS for the remainder of the Term of the Deed. The department requires that your organisation ensure that [redacted] has no further access to ESS or job seekers' records.

Pursuant to clause 52.1(a) of the Deed, the department requires MAX Employment to rectify the abovementioned breach as follows:

1. from the date of this notice:
  - a. ensure that its subcontractors provide privacy and security training to all of their employees with access to ESS which is equal to the training provided by MAX Employment, i.e. at the commencement of employment and at a minimum yearly refresher training, including the completion of annual declaration of interest disclosures which are maintained in a centralised register;
  - b. ensure that all employees and subcontractors complete the relevant IT Security Policy and Information Exchange and Privacy training modules; and
  - c. put in place controls to ensure compliance with the Department's Security Policies; and
2. within 20 business days from the date of this notice:
  - a. develop system controls which restrict their employees and subcontractors access to ESS prior to completion of appropriate training and completion of a declaration of interest disclosure; and
  - b. advise the department of any other steps that have been taken by MAX Employment to mitigate the risk of further breaches.

We require a written report, to be provided to the department, in relation to the implementation of the rectification action outlined above, within 25 business days of the date of this notice.

Should your organisation fail to comply, or comply adequately, with the above required rectification action within the stated timeframes, the Department will be entitled to proceed

3.

to take remedial action under the Deed, including pursuant to clause 52.2. The department reserves all rights under the Deed and at law in regard to this matter.

The department is writing separately to Sureway Employment and Training about this matter to advise them of the termination of \_\_\_\_\_ access to ESS and job seekers' records, and the reinstatement of \_\_\_\_\_ ESS access.

If you have any enquiries in relation to this matter, please contact your Account Manager, \_\_\_\_\_, Providers and Purchasing at \_\_\_\_\_ or telephone (02) 6240 2606.

Yours sincerely ~

Quality and Integrity Group

20 September 2016

Group Manager  
Quality and Integrity Group  
Department of Employment  
GPO Box 9880  
Canberra ACT 2601

October 25<sup>th</sup>, 2016

Dear \_\_\_\_\_

**RE. ESFS-288244**  
**Suspected Unauthorised Access to Departmental Systems —**

I am writing to you today in response to your letter dated 20<sup>th</sup> September regarding unauthorised access to Departmental systems by \_\_\_\_\_ from Sureway who was previously engaged to deliver services on behalf of MAX Employment. In line with your request we wanted to provide the following outline of the rectification actions undertaken.

Please find the following details against specific requirements outlined in your correspondence;

1. from the date of the notice:

- a. ensure its subcontractors provide privacy and security training to all of their employees with access to ESS which is equal to the training provided by MAX Employment, i.e. at the commencement of employment and at a minimum yearly refresher training, including completion of annual declaration of interest disclosures which are maintained in a centralised register;

*MAX Solutions has written to their subcontractor partners and included;*

- *Highlighted the importance of their obligations with IT and Systems security*
- *Re-established requirements for onboarding in line with MAX protocols including the completion of IT Security Policy and Information Exchange and Privacy ECSN training modules at the commencement of employment*
- *Advised them of the requirement to follow up on any backlog of staff who have not completed this training*
- *Offered advice regarding new MAX IT System Security Awareness training and completion of employee interests disclosure for all new starters and for all current staff to complete by a deadline of November 14<sup>th</sup>. The annual requirement of the IT System Security Awareness training and completion of employee interests disclosure to be completed as a refresher has also been highlighted*

*Copies of the communications have been provided as a part of this report including a letter issued specifically to Sureway on 26<sup>th</sup> September regarding their obligations under the subcontract arrangement and upholding ECSN security and other Deed requirements.*



- b. ensure that all employees and subcontractors complete the relevant IT Security Policy and Information Exchange and Privacy training modules; and

*As highlighted previously MAX Solutions has reestablished the requirements for the completion of the relevant IT Security Policy and Information Exchange and Privacy training modules within ECSN. It forms a part of the onboarding responsibilities of all staff who gain access to the ESS system and is noted as a day one priority. We have recently reviewed all outstanding training for MAX staff and associated subcontractors and assigned the two modules to any staff where exceptions exist. Whilst this is being prioritised it should be noted that the introduction and completion of the new IT System Security Awareness training and completion of employee interests disclosure for all new starters and for all current staff to complete by a deadline of November 14<sup>th</sup> has been the key focus and our follow up of any outstanding ECSN modules will be finalised after that date. On a related point the contents of the IT System Security Awareness training have been largely mirrored on the key elements of the ECSN modules themselves. We note that the Information Exchange and Privacy module appears to be somewhat outdated with references to Job Services Australia and will be looking out for any revisions into the future.*

*In line with our commitment to drive the key messages regarding IT System Security we have included a set of key principles and repeated them in the employee interests disclosure requiring staff to agree to them.*

*The measures include;*

- You **must not** share your User ID's and passwords or leave them written down in a location for others to see
- You **must never** use the system for a purpose not authorised by the Department
- You **must not** enter any system record unless you have a direct work related servicing or business requirement
- You **must not** disclose information obtained from Departmental and MAX Systems to someone not authorised to receive it
- You **must not** make any false or fraudulent declaration
- You **must always** 'lock' (Cntrl/Alt/Delete) your computer system when moving away from your workstation regardless of the timeframe involved
- You **must not** attempt to inappropriately obtain increased system access
- You **must immediately** report any instance of inappropriate access or use of the system or data.

- c. put in place controls to ensure compliance with the Department's Security Policies; and

*As you are aware the information security guidelines, required by the Department of Employment, are based on the set of minimum, mandatory requirements set forth in both the Australian Government Protective Security Policy Framework (PSPF) and the Australian Government Information Security Manual (ISM). MAX Solutions is well advanced with its progress to gaining these information security requirements with the aim to gain accreditation and official certification via an InfoSec Registered Assessors Program (IRAP) assessor. MAX is utilising this opportunity to develop and/or refine established policy and procedures to further enhance our compliance to the various IT Security Policies and general requirements as set out in the jobactive Deed 2015-2020.*

*As a starting point MAX Solutions engaged subject matter experts DotSec to complete the SOA-1 gap analysis of MAX Solutions' computing infrastructure and associated processes, policies and procedures, identifying and documenting any areas in which MAX Solutions does not currently comply with SOA-1 requirements.*

---

*The project is being overseen by MAX Solutions Project Management Office and will manage the delivery of the eight SOWs under IRAP Stage 1 to achieve compliance with SOA1 and prepare for SOA-2 from 2 January 2016 to 31 December 2016. The 2017 scope of works will be defined under IRAP Stage 3 which will commence in the second quarter of the 2016 calendar year.*

2. within 20 business days from the date of this notice:

- a. develop system controls which restrict their employees and subcontractors access to ESS prior to completion of appropriate training and completion of a declaration of interest disclosure; and

*MAX Solutions have implemented a new range of system based controls to ensure that all new team members and subcontractors are required to complete the below training before they are able to access ECSN.*

*This training is issued as "System Security Onboarding Training" curriculum by our Learning and Organisational Development (L&OD) team and contains two modules:*

- 1. Information Security and Awareness Training (IRAP) 2016*
- 2. Annual Employee Interests Disclosure Survey 2016*

*New starters are only 'activated' and able to access ESS once L&OD has verified completion of both training modules via the MAXPerform internal database. This measure was introduced on Monday 17<sup>th</sup> October and coincided with the issue of the same training material to every existing MAX Solutions staff member or subcontractor the following day with a requirement to complete both, including a satisfactory pass mark in the IRAP quiz by Monday 15<sup>th</sup> November 2016. This will mark the anniversary date and both modules will be required for completion on an annual refresher basis.*

*Staff that identify any registered job seeker in the interests disclosure are issued separate advice regarding their obligations in the important area of managing conflict of interest including the organisational requirements. Staff are also instructed to provide updates with any changes to their entries in the register and as mentioned before this is programmed to be updated on an annual refresher basis.*

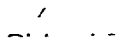
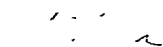
- b. advise the department of any other steps that have been taken by MAX Employment to mitigate the risk of further breaches.

*MAX Solutions adopts the following additional measures to mitigate the risk of further breaches;*

- Launched a new IRAP and System Awareness Training group within the enterprise social network service of Yammer which is being utilised to promulgate key message regarding IT System security and also share best practice with staff*
- Invests significantly in internal training with State based L&OD staff who deliver a range of face to face and webinar based training programs focused on program delivery and compliance with various Federal and State based legislation including IT System Security and Privacy*
- Established a rigorous internal audit program across all employment services and corporate functions with both on-site and desk top audit reviews*
- Provision of help desk facilities for IT and Operational matters based at both National Support Centre and National Operations Centre to support staff working throughout the various MAX Employment offices*
- Probity & Ethics hotline with 24 hour toll free number and email service offering staff the opportunity to escalate any issues in an anonymous manner regarding IT System Security or any contractual or ethical related matter*
- Established Probity Officer and Privacy Officer reporting functions with direct reporting responsibilities to parent company MAXIMUS*
- Involvement of in-house Corporate Counsel working within the MAX Solutions operation allowing us to address legal matters relating to IT System Security and other legislative matters.*

MAX Solutions takes its responsibilities with IT System Security and all other Personal Information highly seriously and are committed to full compliance in this important legal and ethical area. We are happy to provide you further detail and/or clarification of any of the enclosed should you wish.

Yours sincerely



MAX Solutions Pty Ltd

**Attachments:**

- Communication from MAX Solutions re IT System Security to Subcontractor – Sureway*
- Communication from MAX Solutions re IT System Security to Subcontractor – yourtown*
- Communication from MAX Solutions re IT System Security to Subcontractor - Rainbow Gateway*
- Internal communication regarding revised onboarding processes dated 14/10/2016*
- Internal communication regarding required System Security Awareness Training and Employee Interests disclosure survey dated 18/10/2016.*



Australian Government  
Department of Employment

National Office

Your Ref  
Our Ref: ES-15-11035

Serendipity (WA) Pty Ltd  
Pricewaterhouse Coopers building  
Level 15/125-137 St Georges Terrace  
Perth WA 6000

Dear \*

**jobactive Deed 2015-2020 – Unannounced visit findings – Mitchelton site**

I refer to the jobactive Deed 2015-2020 ('the Deed') between Serendipity WA Pty Ltd trading as Advanced Personnel Management (APM) ('Your Organisation') and the Commonwealth, as represented by the Department of Employment ('the Department').

I am writing to you to provide feedback on an unannounced visit at the APM Mitchelton Site that the Department conducted on 16 August 2016. The visit was conducted by [redacted] Contract Managers from the Department's Brisbane office) with [redacted] te Manager of Mitchelton) and (Employment Consultant) in attendance at the Mitchelton Site. As stated in the letter that the Contract Managers provided to [redacted] at the time of the visit, the visit was a programme assurance activity conducted in accordance with clause 27 (Programme Assurance Activities) and clause 40.3 (Access to Premises and Records) of the Deed.

The visit focussed on the areas of site location, facilities, privacy and storage of records. Attachment A details the Contract Managers' relevant findings. Based on these findings, the Department is primarily concerned with the storage of job seeker records and the associated privacy issues at the APM Mitchelton site.

As set out in Attachment B, all jobactive providers have obligations under the Deed and the *Privacy Act 1988* (Cth) to ensure that personal information is collected, held, used and disclosed in accordance with that Act. In addition, the Deed requires providers to store and control access records in accordance with the Records Management Instructions.

The Department treats any failure to comply with these obligations very seriously, regardless of how it occurs. It is important that your organisation take action as soon as possible, to

ensure that privacy of job seekers' information is maintained and job seekers are not adversely affected.

As set out in Attachments A and B, the Department has also identified non-compliance at the Mitchelton site of obligations relating to customer feedback register.

**Action required**

The Department requires your organisation to provide a response, within 10 business days from the date of this letter, outlining what steps that it intends to take to immediately rectify the deficiencies identified at the visit and to reduce the risk of future non-compliance with the Deed. Your response should also identify the timeframe within which these steps will be taken.

The Department reserves the right to take further action it deems necessary under the Deed in relation to your organisation's non-compliance. If your organisation does not respond within the specified timeframe, or your response fails to demonstrate appropriate rectification of the deficiencies outlined, then the Department may choose to take remedial action under the Deed.

If you have any questions regarding the details of this letter, please contact I on (03) 5430 5629 or myself on (02) 6240 2606.

Yours sincerely

Providers and Purchasing Branch  
Quality and Integrity Group

20 October 2016

## Attachment A

### Relevant findings from the unannounced visit of 16 August 2016

The Contract Managers made the following observations:

- s desk had documents exposed on it for a number of different job seekers, not only the job seeker she had just interviewed at her desk.
- A significant number of other job seeker records were stored in an unlocked cupboard and were visible in a small overflowing bin beside the printer.
- advised that staff type notes directly into the system while job seekers are present. Printed records are scanned and then shredded. A number of printed records were seen to be unsecured while waiting for shredding. advised that the site does not have a lockable filing cabinet or lockable file room.
- Contract Managers requested to view the Site Customer Feedback Register. responded that there is no Customer Feedback Register at that site. When asked about APM's complaint management process I advised that complaints are registered 'internally' (on PULSE) and dealt with online through APM's system.

#### Action taken on site

The Site Manager was requested to make immediate arrangements to secure the personal job seeker information on site. subsequently confirmed that this had occurred before the site closed on the same day. The records were transferred to a cupboard and a lock purchased for the cupboard.

## Attachment B

### Deed clauses and legislation non-compliance

Specifically, the Department notes that your organisation has failed to comply with:

- the *Privacy Act 1988* (Cth) ('the Privacy Act'), specifically Australian Privacy Principle (APP) 11 and possibly APP 6;
- clause 35.2 of the Deed in that it failed to comply with the Privacy Act and the APPs as if it were an agency;
- clauses 37.5 and 37.7 of the Deed in that it failed to store and control access to Records in accordance with the requirements of clause 37 and the Records Management Instructions;
- clause 30.5(a) in that it failed to keep a Customer feedback register for the Mitchelton Site;

# employment services

October 27<sup>th</sup> 2016

— Providers and Purchasing Branch  
Quality and Integrity Group

Dear

Re: jobactive Deed 2015–2020 — Unannounced visit findings — Mitchelton site — August 16, 2016  
(Your Ref: ES–15–1103)

I am writing in response to your letter dated 20<sup>th</sup> October 2016 providing feedback regarding the Department's visit to APM's Mitchelton site in August 2016.

APM takes the responsibility to comply with all contractual requirements and maintain appropriate job seeker record storage seriously. We acknowledge that at the time of the Department's visit to the site there were some deficiencies identified, however can advise that these were isolated issues, and that all were immediately rectified and further preventative controls put in place.

In response to the identified issues:

- *desk had documents exposed on it for a number of different job seekers, not only the job seeker she had just interviewed at her desk.*
- *A significant number of other job seeker records were stored in an unlocked cupboard and were visible in a small overflowing bin beside the printer.*
- *! advised that staff type notes directly into the system while job seekers are present. Printed records are scanned and then shredded. A number of printed records were seen to be unsecured while waiting for shredding.*
- *advised that the site does not have a lockable filing cabinet or lockable file room.*

As mentioned in your letter, APM took immediate action on the same day to address these issues, including ensuring that all printed records were transferred to a cupboard with a lock. We also obtained a lockable document disposal bin for the site to ensure there is now no need for document shredding to be managed locally i.e. documents can be immediately disposed of. and staff at the site have also undergone further privacy training.

Subsequent to implementing the above corrective actions, we have also undertaken our own follow up "unannounced visit" at the Mitchelton site to confirm that all changes have been embedded in daily practice. Similar visits to other sites in the Region have further confirmed that correct privacy protocols are being observed.

Further to responding to the issues identified locally at the Mitchelton site, APM is implementing wider initiatives to mitigate the risks of any similar occurrences, including:

- Recently providing all staff with a quick reference "Privacy and Security Guide" to reiterate key daily practice requirements.
- Progressing in line with the requirements and timeframes of the Department's "Statement of Applicability" to ensure Information Security Registered Assessors Program accreditation by 2018.
- Trialling electronic signature pads to determine the effectiveness of these replacing the need for documents to be scanned and destroyed locally. The trial is expected to be completed by the end of November.
- Undertaking our own site visits to confirm compliance with APM and Department privacy protocols (ongoing).



- *Contract Managers requested to view the Site Customer Feedback Register [redacted] responded that there is no Customer Feedback Register at that site. When asked about APM's complaint management process [redacted] advised that complaints are registered 'internally' (on PULSE) and dealt with online through APM's system.*

APM would like to clarify that a Customer Feedback Register is maintained for the Mitchelton site (as it is for all other APM sites). Customer feedback records are managed electronically (as indicated by [redacted] comments that complaints are "registered 'internally' (on PULSE)"). To ensure the integrity of the Registers, these are maintained centrally by our Audit & Compliance Department and not accessible to local staff, hence [redacted] comments on the day. APM's Customer Feedback Register and process is reviewed as part of our ISO 9001 accreditation and has more recently been endorsed as part of our Quality Assurance Framework accreditation. Job seekers are also informed of the feedback process via our APM Job Seeker Handbook (issued to all job seekers). We therefore consider there to be no issue with the Mitchelton Feedback Register.

APM is confident that our Customer Feedback management system is robust and that the actions we have undertaken to address the identified issues at the Mitchelton site have resolved the situation. Our continued monitoring of this across the Region and nationally will ensure ongoing adherence with contractual document storage and privacy requirements.

If you have any queries regarding this response, or should you require any further clarification, please do not hesitate to contact me on 0419 754 653.

Yours sincerely,

[redacted]

[redacted] - Employment Services



Australian Government  
Department of Employment

National Office

Your Ref  
Our Ref: ES-15-11010

The Salvation Army (Victoria) Property Trust  
Level 3 10 Wesley Court  
Burwood East VIC 3151

Via email: -

Dear

**jobactive Deed 2015-2020 – disclosure of unauthorised information**

I refer to the jobactive Deed 2015-2020 ('the Deed') between the Salvation Army (Victoria) Property Trust (ARBN 143 615 169 Incorporated in Victoria) ('Your Organisation') and the Commonwealth, as represented by the Department of Employment ('the Department').

I am writing to you regarding an incident involving the unauthorised disclosure of Department of Human Services (DHS) officer contact information by an employee of your organisation via email on 16 December 2016. The email trail is at Attachment A.

It appears that [redacted] is forwarded an email trail to a job seeker which includes an email received from the DHS Participation Solutions Team, which contains DHS personnel details. It would have been more appropriate for [redacted] to summarise the content and only provide the relevant information to the job seeker instead of forwarding the email from DHS.

**Required Action**

As you are aware, providers must comply with all of their obligations under the Deed, including obligations relating to Personal and Protected Information under clause 35 of the Deed. The Department treats any failure to comply with these obligations very seriously, regardless of how it occurs, and it is important that rectification action is taken, as soon as possible, to prevent incidents of this nature reoccurring.

Clause 35.2(c) of the Deed requires Providers not to do any act or engage in any practice that if done or engaged in by an agency would be a breach of an Australian Privacy Principle (APP) under the *Privacy Act 1988* (Cth) (Privacy Act). Disclosure of DHS staff's personal information to an unauthorised recipient could be considered a breach of the Australian Privacy Principles.

Accordingly, the Department requires your organisation to provide a response by 16 January 2017 explaining why and how this incident occurred and outlining what steps that it intends to take to reduce the risk of future non-compliance with the Deed including the time frames for taking those steps.

The Department reserves the right to take further action it deems necessary under the Deed in relation to your organisation's alleged non-compliance. If your organisation does not respond within the specified timeframe, or your response fails to demonstrate appropriate rectification of the deficiencies outlined, then the Department may choose to take remedial action under the Deed.

If you have any questions regarding the details of this letter, please contact your Account Manager, on (03) 9954 2574 or myself on (02) 6240 2606.

Yours sincerely

Quality and Integrity Group  
23 December 2016

Email: [EmploymentVICJobactive@employment.gov.au](mailto:EmploymentVICJobactive@employment.gov.au)

9 January 2017

Dear ^ ^

**Re: jobactive Deed 2015-2020 – disclosure of unauthorised information**

Thank you for bringing this matter to our attention.

The Salvation Army Employment Plus is committed to upholding the Privacy Principles and take privacy very seriously.

As requested, please see The Salvation Army Employment Plus' response in relation to this matter below.

The Acting Operations Manager has discussed the incident with the staff member involved, and the circumstances leading up to the incident are as follows:

- Job seeker is a self-employed Actor and there have been numerous issues with job seeker's non-attendance and participation in activities
- After the latest compliance action, the job seeker allegedly followed-up the compliance action with DHS and then demanded that the site reverse the Compliance Report
- The staff member contacted the PST in relation to the job seeker's enquiry and obtained a response from PST
- In an attempt to resolve the ongoing issues with this job seeker, the staff member forwarded the email from PST directly to the job seeker
- The staff member stated that he wasn't aware of the PST staff member's details being on the email and apologises for his error.
- The staff member stated that he normally would extract content of a PST email and send it onto a job seeker - without PST staff member's contact information.

**Steps to reduce risk of future non-compliance:**

- The staff member has been instructed that the disclosure of the DHS officer's contact information should not have occurred and that this must not occur in future.
- The staff member has also been directed to complete the Privacy training module again, as well as read and understand the Privacy Principles and Deed Clause 35 by 13 January 2017. The staff member is required to confirm in writing to the Acting Operations Manager that he has completed the required module and read through the relevant documentation.
- Any further breaches by this staff member will result in disciplinary action up to and including termination for any serious breach.
- A message to remind not to disclose Personal and Protected Information without authorisation was included in the latest 'Key Contract Messages' document emailed to staff on Friday 6 January 2017.

 Employment Plus

Should you wish to discuss the matter further or would like additional information please do not hesitate to contact me directly.

Kind regards // /