Australian Government

Department of Employment and Workplace Relations

External Systems Accreditation Authority
A/g First Assistant Secretary – Digital Solutions Division
Adam Shain

Accreditation of the third party employment systems BuddyNote and Performance Reports

This document is to assist employment services providers understand the scope of the accreditation of BuddyNote and Performance Reports performed for the Department of Employment and Workplace Relations (the department). The accreditation assessment has been performed against the Information Security Manual (ISM) March 2023.

Accredited features and benefits

The following features and benefits of BuddyNote (BN) and Performance Reports (PR) have been accredited for use:

Feature	Feature description
Business Functions	- Configurable dashboards: to keep track of key metrics (eg outstanding plans, job seekers with no forward appointments, available claims, caseload numbers, star performance, performance metrics, program metrics) - Performance: KPI analysis, KPI predictive analysis, conversion rates, cohort analysis, outcome rates, target setting and management - Referral Management: Capturing the number and progress of potential referrals through referral sources (service providers), before they are commenced into DES or other program, and before they appear in ES Reporting - Job seekers/ potential job seekers: notes, forms and documents, work preparation progress, job matching, placement tracking, staff performance - Diary and appointment results and management: prompts and reminders for un-resulted ESS diary appointments, making follow up appointments, entering corresponding case notes - Customer Relationship Management (CRM): employers, service providers, marketing lists, lead management, job matching, staff performance, sales management - Internal Staff Communication: notices and alerts within the system - Income: view and compare income across a range of parameters including time frames, geographical area, staff members and claim types.

Feature	Feature description
Job services	- Job seeker management: case notes, work readiness progress, task management, costs, document management, work preferences, lead matching - Employer management: employer notes, sales pipeline, lead management, cost of leads, task management - Live Jobs Board: lead tracking, job seeker referral to leads, staff performance.
Post Placement Support	- Outcome tracking - Available claims - Upcoming claims - Permissible breaks - Verification of work hours and gross income.
Tasks and Activities for service providers	- Internal 'Follow-ups' for job seekers, employers and service providers for any activity - Progress meters for potential job seekers (with customisable task checklists) - Progress meters for work readiness (with customisable task checklists) - Creating notes and attachments to tasks - Alerts for PPS, Compliance activities, Claims, and Marketing.
Customisation	Highly customisable for the customer: - Performance and KPI analysis using any parameters - Dashboard widgets (users can select how to display their dashboards) - Case Note Templates (users can create their own template suite, or select from pre-existing templates) - Employer Note Templates (users can create their own template suite, or select from pre-existing templates) - Documentary Evidence Templates (users can create their own template suite, or select from pre-existing templates to ensure all claims evidence is retained electronically) - Set staff members dollar value per hour.
Mobility and availability	BN and PR are SaaS based application and optimised for multiple device type and size.

Feature	Feature description
Reporting	Specialised Reporting is a key feature of BN and PR – all reports are highly customisable and exportable to multiple file types. Ability to search any Program/ESA/Site/Speciality/Team/Case Manager for analysis and insights, including: - Star rating history and forecast - Outcome rates, including predictive data - Funding level breakdowns/ comparisons - Cohorts - Conversion rates - Trackers - Caseload reporting - Staff performance by caseload - Staff performance by sales - Staff performance by income - Employer insights - Service provider insights - Lead performance - Heat maps displaying locations of metrics (addresses, outcomes, disability types, cohorts).
Administration	A Leading Directions Administrator creates a new customer's Site Administrator(s) (the highest level of access for a customer). Site Administrators cannot manage another Site Administrator's access. Only a Leading Directions Administrator can create or modify a Site Administrator's access. The Site Administrator user undertakes various BN and PR functions including: - Create new users (below Site Administrator) - Manage user access levels (below Site Administrator) - Update user details - Assign user teams and ESAs - Customise dashboards and templates - Create internal notices - View user audit and history data - Merge duplicate records - Archive job seekers, employers or service providers - Modify settings such as Case Note Editing, dollar value per hour. All users can reset their own passwords.
Document Management (BN only)	Documents can be uploaded into BN and managed from all job seeker, employer and service provider records, for the following file types: - csv, xls, xlsx, txt, pdf, doc, docx, jpeg, jpg, png.

Feature	Feature description
Audit Trail	BN and PR audit logs records all: - Caseload searches - Employer/ service provider searches - Job seeker record views - Employer record views - Case notes created, edited and deleted - Employer notes created, edited and deleted - Password resets/ changes - Site Administrator and Administrator user modifications (create account, delete, disable, enable, change name, change ecsn user, change password) - Login details (including failed attempts) - Document access (downloads, upload of documents to JS, Employer, Service Provider, Potential Client).

System security	BN and PR have been designed per Information Security Manual (ISM) March 2023 and is certified against ISO 27001:2013 customised to include the ISM controls. Current configuration includes:
	- The database server is not accessible over the internet
	- Backend/ management access to BN and PR is restricted to named users with multi-factor authentication
	- All connection requests made to BN and PR are filtered through a web application firewall, and suspicious connections are terminated to maintain the confidentiality, integrity and availability of BN and PR.
	All the data stored and processed by BN and PR (e.g., ESS reports, job seeker data, service provider credentials) is protected using ASD approved encryption algorithms:
	  - In transit: using TLS 1.2 connections only
	  - At rest: using AES256 encryption
	BN and PR are hosted in the Australia region of AWS and an office in South Australia.
	Leading Direction's systems are backed up daily, and regular restoration tests are conducted to validate the functionality of the backups.
	By design, BN and PR 'denies' all access requests, unless explicitly allowed.

Provider responsibilities

To use BuddyNote and Performance Reports in an appropriately secure manner, there are actions required on the part of providers.

- Advise the department of your intention to start, expand or cease using BuddyNote or Performance Reports.

- All interactions between Leading Directions and the provider's environment are subject to the provider's own assessment under the Right Fit For Risk assurance approach.

- Leading Directions uses an extension of the shared responsibility model to deliver BuddyNote and Performance Reports. Amazon Web Services (AWS) is responsible for security **of** the cloud; Leading Directions is responsible for security **in** the cloud as well as security **of** the application; the provider is responsible for security **in** the application. This means that it is the provider's responsibility to configure BuddyNote and Performance Reports appropriately to meet their security requirements. Leading Directions have confirmed to the department that they have obtained the Certification Letter and Certification Report issued by the ACSC in relation to AWS, and that they have appropriately addressed the items noted within these documents. Leading Directions informs providers during implementation, and via ongoing training and support, of security requirements and will provide an IT Security Awareness fact sheet.

- User access for provider staff is controlled by provider staff. Providers need to determine what roles are required to allow their staff to perform their jobs while maintaining minimum privileges. Providers are also responsible for the timely removal of BuddyNote and Performance Reports access when their staff no longer require it.

- Forgotten passwords can be securely reset by each user over email. It is the provider's responsibility to positively identify users during enrolment or manual password resets.

- Web application events such as search histories and viewing customer records are logged but do not form part of Leading Direction's event logging strategy. The provider is responsible to perform these security event log audits covering both the provider's own staff and Leading Directions staff activity within BuddyNote and Performance Reports relating to their job seekers.

- Data imported (exported) to BuddyNote is not immediately scanned for malicious and active content. BuddyNote will accept the importation of files in csv, txt, pdf, doc, docx, xlsx, xls, jpg, jpeg and png file types. Attachments are uploaded into an S3 bucket for document storage, where there is no execution. Where a file cannot be scanned by BuddyNote, the user is not presented with a warning that the file has not been scanned. There is reliance on the use of appropriate anti-virus scans and log reviews by the provider and their job seekers using BuddyNote when these documents are downloaded and accessed in their own environments. Providers should perform these monthly audits covering both the provider's own staff and Leading Directions staff importing (exporting) content to BuddyNote relating to their job seekers. Performance Reports does not allow files to be imported.

- When information is introduced onto a system not accredited to handle the information, personnel must not delete the information until advice is sought from an IT Security Manager. BuddyNote and Performance Reports does not currently prevent or detect unaccredited information introduced, or prevent a user deleting it. Providers are responsible for educating their staff as to what should be stored in BuddyNote and Performance Reports and that they are not to delete information until advice has been sought internally.

- When information is introduced onto a system not accredited to handle the information, personnel should not copy, print or email the information. BuddyNote and Performance Reports does not currently prevent or detect unaccredited information introduced, or prevent a user copying, printing or emailing it. Providers are responsible for educating their staff as to what should be stored in BuddyNote and Performance Reports and that they are to pay particular attention to avoid data spillage/ leak when copying, printing or emailing.

- Application logs held within the database will not be retained by Leading Directions following termination of a provider's contract with Leading Directions. It is the provider's responsibility to obtain a copy of the database prior to the termination of their contract and retain as necessary to meet requirements.
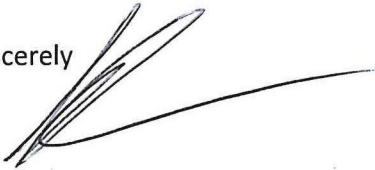
Action plans to address weaknesses

Leading Directions is committed to further strengthening the security of BuddyNote and Performance Reports by the end of the second half of 2023. Specifically, Leading Directions will:

- Develop, implement, and maintain a vulnerability disclosure program including disclosure procedures.
- Host a 'security.txt' file for all internet facing organisational domains to assist in the responsible disclosure of security vulnerabilities in an organisation's products and services.

Leading Directions will provide the department with the results of an independent assessment to support this has been achieved.

Yours sincerely

Adam Shain
30 November 2023