OVIC

Office of the Victorian Information Commissioner

Protective Data Security Plan (PDSP)

Multi-Organisation reporting form (Primary)

Information Security

Victorian Protective Data Security Standards
Reporting information security capability and implementation progress

Version 3.2

This form is intended to be completed electronically.
Different softwares may preview form fields differently.

The 2022 PDSP form was developed using Acrobat 2020 (20.004.30020).
For best results when completing this form, please use a compatible version of Adobe Acrobat Reader or Adobe Acrobat Pro.

Freedom of Information | Privacy | Data Protection

Table of Contents

About the Protective Data Security Plan

What is a Protective Data Security Plan?

A Protective Data Security Plan (**PDSP**) is a document that outlines an organisation's plan to address the Victorian Protective Data Security Standards (**VPDSS** or **Standards**) and elements applicable to the organisation. A PDSP must also address compliance by any contracted service provider of the organisation with the VPDSS to the extent that the provider collects, holds, uses, manages, discloses or transfers public sector information for the organisation.

The 2022 PDSP form serves several purposes. It is designed to:

- help the organisation assess its information security capability;
- summarise the organisation's progress towards the implementation of the Standards; and,
- provide assurance to the Office of the Victorian Information Commissioner (**OVIC**) that the organisation is making progress to improving information security.

The submission of a PDSP to OVIC is a requirement under s89 of the *Privacy and Data Protection Act 2014* (**PDP Act**).

What reporting period is covered by this PDSP and when does it need to be submitted?

When completing the 2022 PDSP, consider the activities undertaken during the 1 July 2020 – 30 June 2022 reporting period. Organisations are expected to submit a copy of a PDSP to OVIC between 1 July - 31 August 2022.

How will the information provided be used?

OVIC has a responsibility to provide Ministers and the public with assurance regarding information security capabilities across government. The information provided in this report will be used as an input in determining progress towards meeting the organisation's information security objectives and will form the basis of reporting back to the organisation, and the Victorian Government including the Victorian Government Chief Information Security Officer.

OVIC will collect some personal information as part of the PDSP submission, including name and contact details of the public sector body Head and nominated contact (Information Security Lead). We will use this information for the purposes of distributing content, collecting feedback, or contacting you about the PDSP.

We will not disclose personal information without consent, except where required to do so by law. For more information about how OVIC's handles personal information, please see OVIC's Privacy Policy.

The OVIC Information Security Unit will:

- use the self-assessed report to help plan its engagement and support activities;
- use information to inform assurance activities;
- provide feedback to organisations based on their submissions; and
- use feedback provided for statistical reporting for the improvement of OVIC resources.

The information provided will be managed in accordance with the protective marking you assign. The contents of this PDSP are exempt from the *Freedom of Information Act 1982 (Vic)*.

Where can I find further information?

Further information about the PDSP can be found in the accompanying resource "**How to: A guide to completing the 2022 Protective Data Security Plan**" available from OVIC's website.

If you have any questions about the PDSP, including how to complete it, please contact OVIC's Information Security Unit via email at security@ovic.vic.gov.au

Part A - Information security self-assessment and implementation plan

Instructions
Each Standard has a number of mandatory fields to complete. For an explanation of the form fields, please refer to the accompanying resource "**How to: A guide to completing the 2022 Protective Data Security Plan**" available from OVIC's website.

OVIC
Office of the Victorian
Information Commissioner

INFORMATION FOR
AGENCIES and BODIES

1300 00 6842 | ovic.vic.gov.au

FREQUENTLY ASKED QUESTIONS

PART A OF THE PDSP FORM

PART B OF THE PDSP FORM

PART C OF THE PDSP FORM

SUBMISSION, NEXT STEPS, AND USEFUL LINKS

How-to: A guide to completing the
2022 Protective Data Security Plan (PDSP)

Freedom of Information | Privacy | Data Protection

Note to auditors
The purpose of the VPDSS is to provide a set of criteria for the consistent application of risk-based practices to manage the security of Victorian government information. Elements are security measures that modify risk.

When auditing against this PDSP, auditors should consider how specific controls are implemented with regard to the organisation's internal and external context; the security value of information; and, any associated risks. Auditors should avoid viewing the implementation of the Elements as a compliance activity and instead focus on the risk management aspects.

Standard 1 – Information Security Management Framework

An organisation establishes, implements and maintains an information security management framework relevant to its size, resources and risk posture.

VPDSS Standard 1 Element Assessment

VPDSS Standard 1 Elements		Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
E1.010	The organisation documents a contextualised information security management framework (e.g., strategy, policies, procedures) covering all security areas.				
E1.020	The organisation's information security management framework contains and references all legislative and regulatory drivers.				
E1.030	The organisation's information security management framework aligns with its risk management framework.				
E1.040	Executive management defines information security functions, roles, responsibilities, competencies and authorities.				
E1.050	Executive management nominates an information security lead and notifies OVIC of any changes to this point of contact.				
E1.060	Executive management owns, endorses and sponsors the organisation's ongoing information security program(s) including the implementation plan.				
E1.070	The organisation identifies information security performance indicators and monitors information security obligations against these.				
E1.080	Executive management commits to providing sufficient resources to support the organisation's ongoing information security program(s).				
E1.090	The organisation sufficiently communicates its information security management framework and ensures it is accessible.				

VPDSS Standard 1 Elements		Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
E1.100	The organisation documents its internal control library that addresses its information security risks.				
E1.110	The organisation monitors, reviews, validates and updates the information security management framework.				

VPDSS Standard 1 Maturity Assessment

Current	2024 Target	2026 Aspiration

Use this space to provide any additional commentary around the organisation's implementation of this Standard (optional) No character limit

Standard 2 – Information Security Value

An organisation identifies and assesses the security value of public sector information.

VPDSS Standard 2 Element Assessment

	VPDSS Standard 2 Elements	Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
E2.010	The organisation's Information Management Framework incorporates all security areas.				
E2.020	The organisation identifies, documents, and maintains its information assets in an information asset register (**IAR**) in consultation with its stakeholders.				
E2.030	The organisation uses a contextualised VPDSF business impact level (**BIL**) table to assess the security value of public sector information.				
E2.040	The organisation identifies and documents the security attributes (confidentiality, integrity, and availability business impact levels) of its information assets in its information asset register.				
E2.050	The organisation applies appropriate protective markings to information throughout its lifecycle.				
E2.060	The organisation manages the aggregated (combined) security value of public sector information.				
E2.070	The organisation continually reviews the security value of public sector information across the information lifecycle.				
E2.080	The organisation manages externally generated information in accordance with the originator's instructions.				
E2.090	The organisation manages the secure disposal (archiving/ destruction) of public sector information in accordance with its security value.				

VPDSS Standard 2 Maturity Assessment

Current	2024 Target	2026 Aspiration

Use this space to provide any additional commentary around the organisation's implementation of this Standard (optional) No character limit

Standard 3 – Information Security Risk Management

An organisation utilises its risk management framework to undertake a Security Risk Profile Assessment to manage information security risks.

VPDSS Standard 3 Element Assessment

	VPDSS Standard 3 Elements	Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
E3.010	The organisation conducts security risk assessments and determines treatment plans in accordance with its risk management framework covering all the processes to manage information security risks including: • Risk identification; • Risk analysis; • Risk evaluation; and, • Risk treatment				
E3.020	The organisation records the results of information security risk assessments and treatment plans in its risk register.				
E3.030	The organisation considers information security risks in organisational planning.				
E3.040	The organisation communicates and consults with internal and external stakeholders during the information security risk management process.				
E3.050	The organisation governs, monitors, reviews, and reports on information security risk (e.g., operational, tactical and strategic through a risk committee (or equivalent, e.g., audit, finance, board, corporate governance)).				

VPDSS Standard 3 Maturity Assessment

Current	2024 Target	2026 Aspiration

Use this space to provide any additional commentary around the organisation's implementation of this Standard (optional) No character limit

Standard 4 – Information Access

An organisation establishes, implements and maintains an access management process for controlling access to public sector information.

VPDSS Standard 4 Element Assessment

	VPDSS Standard 4 Elements	Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
E4.010	The organisation documents an identity and access management policy covering physical and logical access to public sector information based on the principles of least-privilege and need-to-know.				
E4.020	The organisation documents a process for managing identities and issuing secure credentials (registration and de-registration) for physical and logical access to public sector information.				
E4.030	The organisation implements physical access controls (e.g., key management, swipe card access, visitor passes) based on the principles of least-privilege and need-to-know.				
E4.040	The organisation implements logical access controls (e.g., network account, password, two-factor authentication) based on the principles of leastprivilege and need-to-know				
E4.050	The organisation manages the end-to-end lifecycle of access by following provisioning and de-provisioning processes.				
E4.060	The organisation limits the use of, and actively manages, privileged physical and logical access and separates these from normal access (e.g., executive office access, server room access, administrator access).				
E4.070	The organisation regularly reviews and adjusts physical and logical access rights taking into account operational changes.				

VPDSS Standard 4 Maturity Assessment

Current	2024 Target	2026 Aspiration

Use this space to provide any additional commentary around the organisation's implementation of this Standard (optional) No character limit

Standard 5 – Information Security Obligations

An organisation ensures all persons understand their responsibilities to protect public sector information.

VPDSS Standard 5 Element Assessment

	VPDSS Standard 5 Elements	Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
E5.010	The organisation documents its information security obligations and communicates these to all persons with access to public sector information (e.g., policies, position descriptions).				
E5.020	The organisation's information security training and awareness content covers all security areas.				
E5.030	The organisation delivers information security training and awareness to all persons with access to public sector information, upon engagement and at regular intervals thereafter in accordance with its training and awareness program and schedule.				
E5.040	The organisation provides targeted information security training and awareness to persons in high-risk functions or who have specific security obligations (e.g., executives, executive assistants, procurement advisors, security practitioners, risk managers).				
E5.050	The organisation reviews and updates the information security obligations of all persons with access to public sector information.				
E5.060	All persons with access to public sector information acknowledge their information security obligations at least annually (e.g., during performance development discussions, attending security briefings, completing security training).				
E5.070	The organisation monitors, reviews, validates, and updates its information security training and awareness program and schedule.				

VPDSS Standard 5 Maturity Assessment

Current	2024 Target	2026 Aspiration

Use this space to provide any additional commentary around the organisation's implementation of this Standard (optional) No character limit

Standard 6 – Information Security Incident Management

An organisation establishes, implements and maintains an information security incident management process and plan relevant to its size, resources and risk posture.

VPDSS Standard 6 Element Assessment

	VPDSS Standard 6 Elements	Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
E6.010	The organisation documents and communicates processes and plan(s) for information security incident management covering all security areas.				
E6.020	The organisation articulates roles and responsibilities for information security incident management.				
E6.030	The organisation's information security incident management processes and plan(s) contain the five phases of: · Plan and prepare; · Detect and report; · Assess and decide; · Respond (contain, eradicate, recover, notify); and, · Lessons learnt.				
E6.040	The organisation records information security incidents in a register.				
E6.050	The organisation's information security incident management procedures identify and categorise administrative (e.g., policy violation) incidents in contrast to criminal incidents (e.g., exfiltrating information to criminal associations) and investigativehandover.				
E6.060	The organisation regularly tests (e.g., annually) its incident response plan(s).				

VPDSS Standard 6 Maturity Assessment

Current	2024 Target	2026 Aspiration

Use this space to provide any additional commentary around the organisation's implementation of this Standard (optional) No character limit

Standard 7 – Information Security Aspects of Business Continuity and Disaster Recovery

An organisation embeds information security continuity in its business continuity and disaster recovery processes and plans.

VPDSS Standard 7 Element Assessment

	VPDSS Standard 7 Elements	Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
E7.010	The organisation documents and communicates business continuity and disaster recovery processes and plans covering all security areas.				
E7.020	The organisation identifies and assigns roles and responsibilities for information security in business continuity and disaster recovery processes and plans.				
E7.030	The organisation regularly tests (e.g., annually) its business continuity and disaster recovery plan(s).				

VPDSS Standard 7 Maturity Assessment

Current	2024 Target	2026 Aspiration

Use this space to provide any additional commentary around the organisation's implementation of this Standard (optional) No character limit

Standard 8 – Third Party Arrangements

An organisation ensures that third parties securely collect, hold, manage, use, disclose or transfer public sector information.

VPDSS Standard 8 Element Assessment

VPDSS Standard 8 Elements		Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
E8.010	The organisation's information security policies, procedures and controls cover the entire lifecycle of third-party arrangements (e.g., contracts, MOUs and information sharing agreements).				
E8.020	The organisation includes requirements from all security areas in third party arrangements (e.g., contracts, MOUs and information sharing agreements) in accordance with the security value of the public sector information.				
E8.030	The organisation undertakes an information security risk assessment of the third party's service offering and addresses any residual risks prior to finalising the arrangement.				
E8.040	The organisation identifies and assigns information security roles and responsibilities in third party arrangements (e.g., contracts, MOUs and information sharing agreements).				
E8.050	The organisation establishes, maintains, and reviews a register of third-party arrangements (e.g., contracts, MOUs and information sharing agreements).				
E8.060	The organisation monitors, reviews, validates, and updates the information security requirements of third-party arrangements and activities.				
E8.070	The organisation documents its information release management requirements (e.g., social media, news, DataVic).				
E8.080	The organisation manages the delivery of maintenance activities and repairs (e.g., on-site, and off-site).				
E8.090	The organisation applies appropriate security controls upon completion or termination of a third-party arrangement (e.g., contracts, MOUs and information sharing agreements).				

VPDSS Standard 8 Maturity Assessment

Current	2024 Target	2026 Aspiration

Use this space to provide any additional commentary around the organisation's implementation of this Standard (optional) No character limit

Standard 9 – Information Security Reporting to OVIC

An organisation regularly assesses its implementation of the Victorian Protective Data Security Standards (**VPDSS**) and reports to the Office of the Victorian Information Commissioner (**OVIC**).

VPDSS Standard 9 Element Assessment

	VPDSS Standard 9 Elements	Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
E9.010	The organisation notifies OVIC of incidents that have an adverse impact on the confidentiality, integrity, or availability of public sector information with a business impact level (**BIL**) of 2 (limited) or higher.				
E9.020	The organisation submits its Protective Data Security Plan (**PDSP**) to OVIC every two years.				
E9.030	Upon significant change, the organisation submits its reviewed PDSP to OVIC.				
E9.040	The organisation annually attests to the progress of activities identified in its PDSP to OVIC.				

VPDSS Standard 9 Maturity Assessment

Current	2024 Target	2026 Aspiration

Use this space to provide any additional commentary around the organisation's implementation of this Standard (optional) No character limit

Standard 10 – Personnel Security

An organisation establishes, implements and maintains personnel security controls addressing all persons continuing eligibility and suitability to access public sector information.

VPDSS Standard 10 Element Assessment

	VPDSS Standard 10 Elements	Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
E10.010	The organisation's personnel security policies and procedures address the personnel lifecycle phases of: • Pre-engagement (eligibility and suitability); • Engagement (ongoing and re-engagement); and, • Separating (permanently or temporarily).				
E10.020	The organisation verifies the identity of personnel, revalidates, and manages any changes as required.				
E10.030	The organisation undertakes pre-engagement screening commensurate with its security and probity obligations and risk profile.				
E10.040	The organisation manages ongoing personnel eligibility and suitability requirements commensurate with its security and probity obligations and risk profile.				
E10.050	The organisation manages personnel separating from the organisation commensurate with its security and probity obligations and risk profile.				
E10.060	The organisation develops security clearance policies and procedures to support roles requiring high assurance and/ or handling security classified information.				
E10.070	The organisation undertakes additional personnel screening measures commensurate with the risk to support roles requiring high assurance and/ or handling security classified information.				
E10.080	The organisation actively monitors and manages security clearance holders.				

VPDSS Standard 10 Maturity Assessment

Current	2024 Target	2026 Aspiration

Use this space to provide any additional commentary around the organisation's implementation of this Standard (optional) No character limit

Standard 11 – Information Communications Technology (ICT) Security

An organisation establishes, implements and maintains Information Communications Technology (**ICT**) security controls.

VPDSS Standard 11 Element Assessment

VPDSS Standard 11 Elements		Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
E11.010	The organisation manages security documentation for its ICT systems (e.g., system security plans).				
E11.020	The organisation manages all ICT assets (e.g., on-site, and off-site) throughout their lifecycle.				
E11.030	The organisation conducts a security assessment for authorising systems to operate prior to transmitting, processing, or storing public sector information.				
E11.040	The organisation undertakes risk-prioritised vulnerability management activities (e.g., patch management, penetration testing, continuous monitoring systems).				
E11.050	The organisation documents and manages changes to ICT systems.				
E11.060	The organisation manages communications security controls (e.g., cabling, telephony, radio, wireless networks).				
E11.070	The organisation verifies the vendors security claims before implementing security technologies.				
E11.080	The organisation manages security measures (e.g., classification, labelling, usage, sanitisation, destruction, disposal) for media.				
E11.090	The organisation manages standard operating environments (**SOEs**) for all ICT assets, including end user access devices (e.g., workstations, mobile phones, laptops), network infrastructure, servers, and Internet of Things (**IoT**) commensurate with security risk.				

VPDSS Standard 11 Elements		Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
E11.100	The organisation manages security measures for email systems.				
E11.110	The organisation logs system events and actively monitors these to detect potential security issues (e.g., intrusion detection/ prevention systems (**IDS/ IPS**)).				
E11.120	The organisation uses secure system administration practices.				
E11.130	The organisation designs and configures the ICT network in a secure manner (e.g., segmentation, segregation, traffic management, default accounts).				
E11.140	The organisation manages a process for cryptographic keys (e.g., disk encryption, certificates).				
E11.150	The organisation uses cryptographic controls for confidentiality, integrity, non-repudiation, and authentication commensurate with the risk to information.				
E11.160	The organisation manages malware prevention and detection software for ICT systems.				
E11.170	The organisation segregates emerging systems from production systems (e.g., physical and/ or logical) until their security controls are validated.				
E11.180	The organisation manages backup processes and procedures (e.g., schedule, isolation, storage, testing, retention).				
E11.190	The organisation manages a secure development lifecycle covering all development activities (e.g., software, web-based applications, operational technology (Supervisory Control and Data Acquisition/ Industrial Control Systems (**SCADA/ICS**)).				
E11.200	The organisation manages security measures for enterprise mobility (e.g., mobile device management, working from home).				

VPDSS Standard 11 Maturity Assessment

Current	2024 Target	2026 Aspiration

Use this space to provide any additional commentary around the organisation's implementation of this Standard (optional) No character limit

Standard 12 – Physical Security

An organisation establishes, implements and maintains physical security controls addressing facilities, equipment and services.

VPDSS Standard 12 Element Assessment

VPDSS Standard 12 Elements	Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
E12.010　The organisation plans and documents physical security measures.				
E12.020　The organisation applies defence-in-depth physical security measures.				
E12.030　The organisation selects physical security measures commensurate with the business impact level of the information.				
E12.040　The organisation has scalable physical security measures ready for activation during increased threat situations.				
E12.050　The organisation implements physical security measures when handling information out of the office.				
E12.060　The organisation manages physical security measures throughout their lifecycle.				

VPDSS Standard 12 Maturity Assessment

Current	2024 Target	2026 Aspiration

Use this space to provide any additional commentary around the organisation's implementation of this Standard (optional) No character limit

Part B - Agency Head Executive Summary (Primary)

Name of public sector agency or body (primary organisation)

Public sector body Head

(e.g., Department Secretary, CEO)

Full Name

Position Title

Phone Number

Email Address

Postal Address

Information Security Lead

(The organisation's nominated contact regarding the VPDSS)

Same as public sector body Head

(Check box optional)

Full Name

Position Title

Phone Number

Email Address

Postal Address

In which part of the organisation does the ongoing management of the information security program reside?

Name of the Victorian government portfolio in which the organisation operates

Security program executive summary from the past 24 months Character limit 2,500

Challenges or barriers

Please select any challenges or barriers that may be inhibiting implementation of the Standards.

Financial

Resourcing

Capability

Legislative

Significant change

External third-party dependencies

Machinery of Government

Lack of clarity around roles and responsibilities within the organisation

Lack of understanding of the Standards

Other (please elaborate below)

Please describe any challenges of barriers towards the implementation of the Standards Character limit 1,000

Organisation Profile Assessment - Primary Organisation

This section assists OVIC's understanding of the primary organisation's security profile.

Number of employees within the organisation	Full-Time Equivalent	Contractors	Volunteers

Does the organisation have Industrial Automation and Control Systems (**IACS**)?
Does the organisation obtain, generate, receive or hold information at Business Impact Level (**BIL**) 3 or higher?

Provide an approximate protective marking breakdown of the organisation's information assets:

BIL 1 (Confidentiality)	**OFFICIAL**	%
BIL 2 (Confidentiality)	**OFFICIAL: Sensitive**	%
BIL 3 (Confidentiality)	**PROTECTED**	%
BIL 3-4 (Confidentiality)	**[security classification]// Cabinet-In-Confidence**	%
BIL 4 (Confidentiality)	**SECRET**	%
BIL 5 (Confidentiality)	**TOP SECRET**	%
Percentage of information not assessed		%
Percentage of information marked using a former scheme or different scheme		%
Total information assets		

Information Security Incidents	How many information security incidents were recorded in the organisation's internal incident register over the last 24 months?
	Of these incidents, how many affected information assets of a BIL 2 or higher?
Third-Party Arrangements	How many third-party arrangements currently have direct access to the organisation's information and information systems?
	What is the highest protective marking that third parties are accessing?

How did the organisation validate the PDSP prior to submission to OVIC?			
Internal Audit	External Audit	Self-Assessed	Other

Part C - Attestation (Primary)

Attestation

Under Part 4 of the *Privacy and Data Protection Act 2014* (PDP Act) and Standard 9 of the Victorian Protective Data Security Standards 2.0 (the Standards), I   , attest that:

- I am the public sector body Head of   (my organisation).

- My organisation has implemented the key activities or is in the process of planning and implementing key activities as required by the Standards.

- My organisation has undertaken a security risk profile assessment or is in the process of undertaking a security risk profile assessment required under section 89 of the PDP Act.

- The organisation(s) listed in **Part D** have implemented the key activities or is/are in the process of planning and implementing key activities required by the Standards.

- The organisation(s) listed in **Part D** have undertaken a security risk profile assessment as required under section 89 of the PDP Act.

Check this box to populate the attestation with details for the **public sector body Head** as listed in Part B of the PDSP.   (Check box optional)

Insert signature here

Print name:

Position:

Date:

Part D - Multi-Organisation Attestation List

The following subsidiary organisations are being attested for under **Part C**.

Name of Public Sector Agency or Body	Name of Public Sector Body Head	The subsidiary is aware of the attestation being made
ISU edit PDF to insert subsidiary entity name	*ISU edit PDF to insert subsidiary head name*	(Check box)
ISU edit PDF to insert subsidiary entity name	*ISU edit PDF to insert subsidiary head name*	(Check box)
ISU edit PDF to insert subsidiary entity name	*ISU edit PDF to insert subsidiary head name*	(Check box)
ISU edit PDF to insert subsidiary entity name	*ISU edit PDF to insert subsidiary head name*	(Check box)
ISU edit PDF to insert subsidiary entity name	*ISU edit PDF to insert subsidiary head name*	(Check box)
ISU edit PDF to insert subsidiary entity name	*ISU edit PDF to insert subsidiary head name*	(Check box)
ISU edit PDF to insert subsidiary entity name	*ISU edit PDF to insert subsidiary head name*	(Check box)
ISU edit PDF to insert subsidiary entity name	*ISU edit PDF to insert subsidiary head name*	(Check box)
ISU edit PDF to insert subsidiary entity name	*ISU edit PDF to insert subsidiary head name*	(Check box)
ISU edit PDF to insert subsidiary entity name	*ISU edit PDF to insert subsidiary head name*	(Check box)
ISU edit PDF to insert subsidiary entity name	*ISU edit PDF to insert subsidiary head name*	(Check box)
ISU edit PDF to insert subsidiary entity name	*ISU edit PDF to insert subsidiary head name*	(Check box)
ISU edit PDF to insert subsidiary entity name	*ISU edit PDF to insert subsidiary head name*	(Check box)
ISU edit PDF to insert subsidiary entity name	*ISU edit PDF to insert subsidiary head name*	(Check box)
ISU edit PDF to insert subsidiary entity name	*ISU edit PDF to insert subsidiary head name*	(Check box)
ISU edit PDF to insert subsidiary entity name	*ISU edit PDF to insert subsidiary head name*	(Check box)
ISU edit PDF to insert subsidiary entity name	*ISU edit PDF to insert subsidiary head name*	(Check box)
ISU edit PDF to insert subsidiary entity name	*ISU edit PDF to insert subsidiary head name*	(Check box)
ISU edit PDF to insert subsidiary entity name	*ISU edit PDF to insert subsidiary head name*	(Check box)
ISU edit PDF to insert subsidiary entity name	*ISU edit PDF to insert subsidiary head name*	(Check box)