SASI AUTONOMOUS
INSTITUTE OF TECHNOLOGY & ENGINEERING
TADEPALLIGUDEM
WEST GODAVARI DIST.,A.P

KEEP DATA SECURE IN A RECRUITING APP

PRESENTED BY:

G Harshitha (19K61A1215)

LECTURER IN CHARGE:

Dr.A.V.N.CHANDRA SEKHAR

PROFESSOR

SITE

Contents

1. Abstract
2. Introducion
3. Literature Survey
4. Methodology
5. Sharing Settings
6. Security Overview
7. Result
8. Conclusion

Abstract

Updates field-level security and create permission sets in an HR recruiting app so that sensitive data can be viewed only by those who need it,also restricts the data access in app by changing sharing settings.

Introduction

- We can continue customizing Computing’s Recruiting app, which the HR team uses as they work to place applicants into open positions in the company,lets consider a example a companys

- Due to popularity recruiting apps are only accessed by authorized persons to ensure the right minds get right operation

Literature Survey

- In 2021 Sarojini et.al proposed a technique known as Enhanced Mutual Trusted Access ControlAlgorithm (EMTACA). This technique presents a mutual trust for both cloud users and cloud serviceproviders to avoid security related issues in cloud computing. The results of this paper showed data confidentiality, integrity and availability which is the three most important aspect of datasecurity was achieved.

- In 2021, Dimitra A. Geogiou wrote a paper to present security policies for cloud computing. The purpose of the security policies is to protect people and information, set rules for expected behavior by users, minimize risks and help to track compliance with regulation.This paper scrutinized the security requirements of a cloud service provider taking into consideration Case study of E-health system of Europe.

Methodology

- **Create Profile:** Before creating the new profile, customize how profiles are viewed. From Setup enter User Management Settings in the Quick Find box, and select User Management Settings,Set Enhanced Profile User Interface to Disabled,Now create an HR Recruiter profile and set its object permissions,From Setup enter Profiles in the Quick Find box, and select Profiles. From the list of profiles, find Standard User. Click Clone.For Profile Name, enter HR Recruiter.Click Save.While still on the HR Recruiter profile page, then click Edit.Scroll down to Custom Object Permissions and change the Basic Access for each object to reflect the table below.

- Permission sets grant additional permissions to specific users, on top of their existing profile permissions, without having to modify existing profiles, create new profiles, or grant an administrator profile where it's not necessary.

Methodology...

- **Create a new permission set for hiring managers** Click Save. Click Assigned Apps in the Apps section, then click Edit. Select Recruiting from the Available Apps list and click Add.

- From Setup, enter Permission Sets in the Quick Find box, and select Permission Sets. Click New, and enter the details. Field Label: Hiring Manager Description: Temporary permission set for those Hiring Managers that need to interview candidates for positions in their department.

Sharing Settings

- Ling Wu would like job postings to be the only HR custom object with public access. Achieve this by changing the organization-wide default sharing settings.

- From Setup, enter Sharing Settings in the Quick Find box and select Sharing Settings. Click Edit in the Organization-Wide Defaults section. Select Private for the Candidate object. Select Private for the Interviewer object. Select Private for the Job Application object. Select Public Read Only for the Job Posting Site object. Select Private for the Position object. Click Save.

- By creating a custom profile, creating permission sets, updating field-level security, and modifying organization-wide default sharing settings, you've made AW Computing's recruiting app a more secure tool. Ling Wu can rest easy knowing that her team—and anyone else accessing the app—will only see the data they're authorized to see.

Security Overview

There are four key issues in the security of databases just as with all security systems

- Availability
- Authenticity
- Integrity
- Confidentiality

Security Overview...

AVAILABILITY

Data needs to be available at all necessary times

- Data needs to be available to only the appropriate users
- Need to be able to track who has access to and who has accessed what data

Security Overview...

AUTHENTICITY

- Need to ensure that the data has been edited by an authorized source
- Need to confirm that users accessing the system
- Need to confirm that users accessing the system are who they say they are need to verify that all report requests are from authorized users
- Need to verify that any outbound data is going to the expected receiver

Security Overview...

INTEGRITY

- Need to verify that any external data has the correct formatting and other metadata
- Need to verify that all input data is accurate and verifiable
- Need to ensure that data is following the correct work flow rules for your institution/corporation
- Need to be able to report on all data changes and who authored them to ensure compliance with corporate rules and privacy laws.

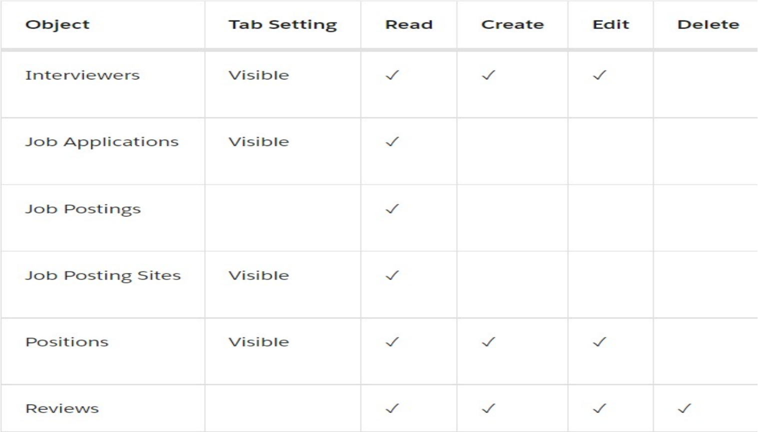
Security Overview...

CONFIDENTIALITY

- Need to ensure that confidential data is only available to correct people
- Need to ensure that entire database is security from external and internal system breaches
- Need to provide for reporting on who has accessed what data and what they have done with it
- Mission critical and Legal sensitive data must be highly security at the potential risk of lost business and litigation

Result

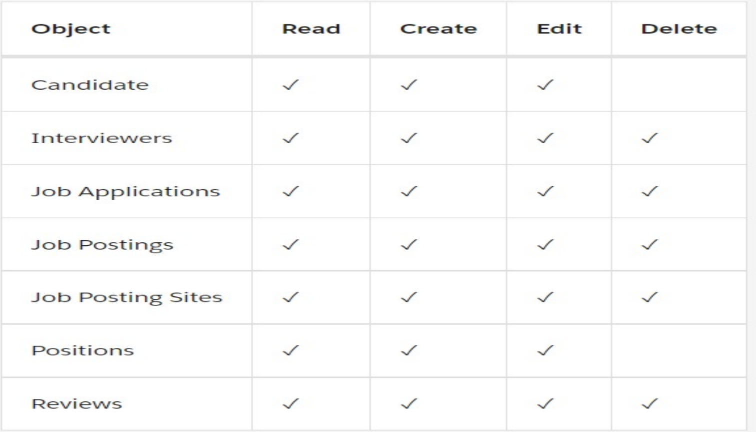
- **Modify Field-Level Security**



Object	Tab Setting	Read	Create	Edit	Delete
Interviewers	Visible	✓	✓	✓	
Job Applications	Visible	✓			
Job Postings		✓			
Job Posting Sites	Visible	✓			
Positions	Visible	✓	✓	✓	
Reviews		✓	✓	✓	✓

Result...

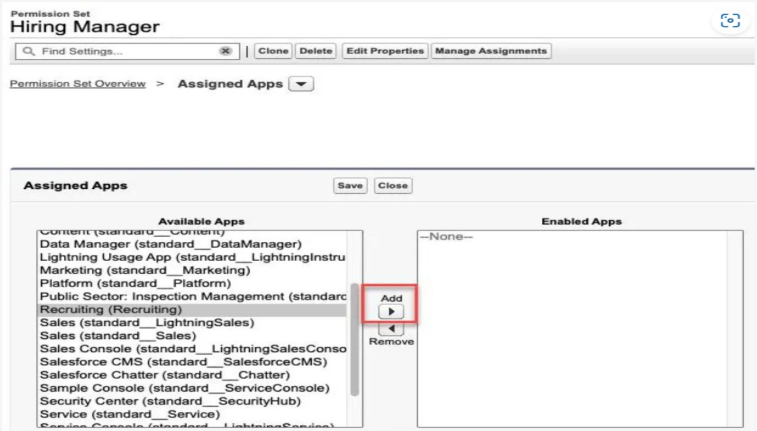
- **Profiles**



Object	Read	Create	Edit	Delete
Candidate	✓	✓	✓	
Interviewers	✓	✓	✓	✓
Job Applications	✓	✓	✓	✓
Job Postings	✓	✓	✓	✓
Job Posting Sites	✓	✓	✓	✓
Positions	✓	✓	✓	
Reviews	✓	✓	✓	✓

Result...

- Assigned Apps in Recruiting form



Permission Set

Hiring Manager

Permission Set Overview > Assigned Apps

Assigned Apps

Available Apps

Content (standard__Content)
Data Manager (standard__DataManager)
Lightning Usage App (standard__LightningInstru
Marketing (standard__Marketing)
Platform (standard__Platform)
Public Sector: Inspection Management (standarc
Recruiting (Recruiting)
Sales (standard__LightningSales)
Sales (standard__Sales)
Sales Console (standard__LightningSalesConso
Salesforce CMS (standard__SalesforceCMS)
Salesforce Chatter (standard__Chatter)
Sample Console (standard__ServiceConsole)
Security Center (standard__SecurityHub)
Service (standard__Service)
Service Console (standard__LightningService)

Enabled Apps

--None--

Result...

- In order to access a record, users must have the appropriate object permission on their profile or a permission set. By changing sharing settings from the organization-wide defaults, you set the default level of access users have to records they do not own in each object.

- Successfully implemented the organization-wide defaults for Recruiting app objects.

Conclusion

- In a global, digital world, the most important currency for any business is trust,trust is something you earn over many years by diligently safeguarding your customer's personal data. They trust you with a lot of essential information – their address, their payment details, their preferences, even their bio metric data.
- It starts with strategy, with people and with education. But the most important part is getting the infrastructure right. A good ETL vendor can help you build a secure data pipeline that keeps sensitive information out of the wrong hands. Your customers will rest easy knowing their personal data is safe.

ANY QUERIES?

THANK YOU!