Campus Consortium's
Password Manager &
Multi-Factor Authentication Grant

Last Date to Apply
August 31st 2018
Overview

Manual password reset is a very common problem in many Institutions. The amount of calls that the IT helpdesk receives can skyrocket not just shooting up helpdesk costs but also keeping them waiting for a long time until their passwords are manually reset.

Password Manager is a Self-Service Password Reset tool that lets your end users recover their accounts and passwords without having to call the IT help desk. This not only cuts short the time they get access to the portal but, also helps save a lot of help desk costs. In addition to it, you could completely get rid of 'default passwords' by helping First-time users set up their accounts, passwords and security questions on their own. Multifactor Authentication is a capability that helps authenticate using more than one factor.

Multifactor Authentication is a boon to IT teams in times like these when there are widespread network security breaches arising due to unauthorized access and insider threats. Role-based Multifactor Authentication & Multifactor Authentication at the time of login are some important features that help you protect your IT resources from unauthorized access.

Considering almost 20% calls to the IT helpdesk is related to password resets. This has led institutions with the following challenges:

1. **Increases Helpdesk Costs**: According to Gartner, $20 is the cost of each manual password reset done through the IT helpdesk.

2. **After-hours Password Reset**: Users would face serious challenges to reset their passwords during the hours when the helpdesk is not operational.

3. **Waiting Time**: There is a wait time associated with getting to the IT helpdesk depending on the number of users wanting to reach them and the number of agents servicing requests.

Campus Consortium's Grant in collaboration with technology partner Quicklaunch puts an end to these problems through awarding a Self-Service Password Manager which lets users reset their passwords through the web interface using Email, Phone and Security Questions.

To bolster IT security, campuses can deploy Multi-Factor Authentication using QuickLaunch Multi-Factor Authentication, which is AI-based, where users are authenticated using multiple modes such as Phone, Email.
Why is Password Manager and Multi-Factor Authentication essential to Campuses?

To deliver uninterrupted access to essential applications without the dependency on the IT helpdesk, campuses automate password resets. It not only gives students instant access to their accounts through self-service password reset but also frees the IT helpdesk thereby delivering considerable IT cost savings. Multi-Factor Authentication (MFA) is a security reinforcement that ensures that there is no room for intruder and the authentication is strengthened by using additional factors.

Key Components of the Grant:

- The cumulative grant reward of $20,000 for over a period of 5 years, covers 100% of the implementation and setup cost
- Multi-Factor Authentication up to 3 factors for 300 users
- Discounted price for additional users
- Multi-year discounts: More discounts when you sign multi-year deals through the grant program.

Password Manager

- Named User
- Active Session Licenses: 100 Active Sessions

QuickLaunch Identity: Basic Support

Multifactor Authentication

- Choose up to 3 SSO Applets
- Customize Security Questions
- Basic Support via Self Help Forum

QuickLaunch Identity Professional Services

QuickLaunch Password Manager Implementation
QUALIFICATION CRITERIA

1. Applicant must be an education institution or public-sector organization.

2. Applicant demonstrates a commitment to implementing the solution (e.g. letter from president highlighting the problem that the solution solves and why the grant would be helpful in meeting strategic objectives).

HOW TO APPLY

1. Download and fill the grant application form

2. Submit grant applications to grantapplication@campusconsortium.org by 5:00 pm ET on August 31st, 2018

GRANT PROCESS

1. Applications Open on August 15th, 2018

2. Apply for the Grant by August 31st, 2018

3. Review of Application by Grant Review Committee by September 05th, 2018

4. Grant Award Letter issued to Grant Recipients by September 10th, 2018

5. Grant Award Walkthrough by September 17th, 2018

6. Execution of Grant Award Agreement by September 24th, 2018

7. Project Kick-Off by October 08th, 2018
### General Information

**Applicant Information**
- **Name of Institution:**
- **President/Chancellor:**
- **Point of Contact:**
- **POC Phone:** **POC Email:**
- **CIO/VP of IT:**
- **CIO Phone:** **CIO Email:**
- **Institution’s Address:**

**IN THE CASE OF BEING AWARDED THIS GRANT:**
- Do we have your permission to email the grant award letter to the President/Chancellor listed above?

If not, please indicate to whom this award should be made out to:

**Media/Communications Contact (for News Release):**

### ENROLLMENT INFORMATION

<table>
<thead>
<tr>
<th>Total Enrollment</th>
<th>Full Time Enrollment</th>
<th>Part Time Enrollment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total # On-Campus Students</td>
<td>Total # Off-Campus Students</td>
<td></td>
</tr>
<tr>
<td># Faculty</td>
<td># Tenured Faculty</td>
<td># of Academic Depts.:</td>
</tr>
<tr>
<td>Alumni Population</td>
<td>% of Alumni Who Donate</td>
<td></td>
</tr>
</tbody>
</table>

If so, approximated how many students does this program serve?

### PLEASE MARK “X” NEXT TO ALL THAT APPLY

- **Public:**
- **Private:**
- **Four-year:**
- **Two-year:**
- **Undergraduate:**
- **Graduate:**

### TECHNOLOGY RESOURCES

*Please indicate all major software being utilized on campus*

<table>
<thead>
<tr>
<th>Enterprise Applications</th>
<th>Vendor &amp; Version</th>
<th>Hosted/On-Site</th>
<th>URL – Enterprise Web App (if available)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Student Information System/Enterprise Resource Planning</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Learning Management System</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Directory System</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**PLEASE ANSWER THE FOLLOWING QUESTIONS:**

How did you hear about this grant?

Do you have current SSO? If Yes, provide a list of all the SSO’s you have

Is the SSO design responsive? List the Vendor Name?

Do you have a timeline for when you would need Single Sign-On live for your institution?

**SIGNATURES**

I authorize the verification of the information provided on this form.

Signature of applicant: ______________________  Date: ______________________