Identity Access and Management Web Site

1. **Introduction**
   1. The Identity and Access Management (IDM) division is responsible for a vast array of employee maintenance actions in order to maintain an accurate access management environment.
   2. Many of these responsibilities rely on separate utilities working in unison to knit these actions together.
   3. The Identity Access and Management Web Site provides a ***One Stop Shopping*** platform to seamlessly tie these separate utilities together behind easy to use User Interface displays.
   4. The services provided within this site will be discussed in section II of this document.
   5. Access to the IDM Web Site can be achieved by clicking [here](http://idmgmtapp01.universal.co) or navigating to http://idmgmtapp01.universal.co
2. **Usage Overview**
   1. The majority of people who visit this site will do so with an intent that can be broken down into two categories:
      1. Informational
         1. Examples would be reviewing:
            1. HR contact information
            2. Master contact lists
            3. Departmental manning reports.
      2. Applications
         1. Examples would be executing:
            1. Terminating employees
            2. Adding new people into Active Directory
            3. Providing managers and other delegated personnel access to recently terminated Associate’s One-Drive accounts.
         2. All application are located within the **Admin Portal** portion of the website which is discussed below.
3. **Admin Portal**
   1. This is a secure area where only authorized who have access can perform applications listed in section II of this document.
   2. To gain access to the Admin Portal, the follow steps must take place:
      1. An invitation must be sent from the web site administration team to the individual requesting access.
      2. That individual will receive that invitation in the form of an e-mail.
      3. Once that individual clicks on the Register link located in the E-Mail, they will be forwarded to the registration area.
      4. Once registered, each user will be assigned an access level.
      5. These access levels control what applications each user has visibility into.
4. **Security**
   1. All associates who are granted access to the Admin Portal are passed an encrypted key to their computer which can only be deciphered by the Web Server.
   2. These encrypted key codes on their own are useless if obtained by an individual hacking into the laptop.
   3. Upon each login, a new encrypted key is regenerated and passed to the client’s laptop.
   4. If any suspicious behavior is observed, that individuals access to the web applications can immediately be suspended.
5. **Logging of Events**
   1. All actions performed within the Admin Portal are logged into a database table.
   2. Information within this table includes:
      1. Name and employee ID of individual who performed the work.
      2. Time the work are executed.
      3. Description of what work was performed.
      4. These logs can be easily reviewed at any time by the administrators of the web site.

*The Main Page of the IDM Web Site*A person touching a touch screen

Description automatically generated with low confidence