



WEBMI & SECURITY

White Paper



THE SIGNIFICANCE OF SECURITY

While Horner Automation software has long been of high quality, the availability and shift in technology toward connected devices and the Internet of Things has led us to double our software efforts to provide the best possible user experience and value.

Horner's WebMI, which works with Cscape for direct remote access to individual Horner OCS units through a web browser on any device a customer chooses. WebMI is just the first part of our web-based features that will expand to include even more interconnected and cloud-based ecosystem we call Web OCS.

Knowledge throughout the industry is being integrated in applications and data in the form of algorithms, closed-loop control parameters and recipes. New opportunities arise from new services such as online monitoring and maintenance that require secure communication and access level control.

With all of this comes an unfortunate, but very real security risk faced by the entire industry. Some malicious actors hack into systems causing countless losses in downtime and recovery costs. Ultimately, operators must protect their intellectual property from unauthorized modifications, access or misuse by third parties to ensure the integrity of their processes.

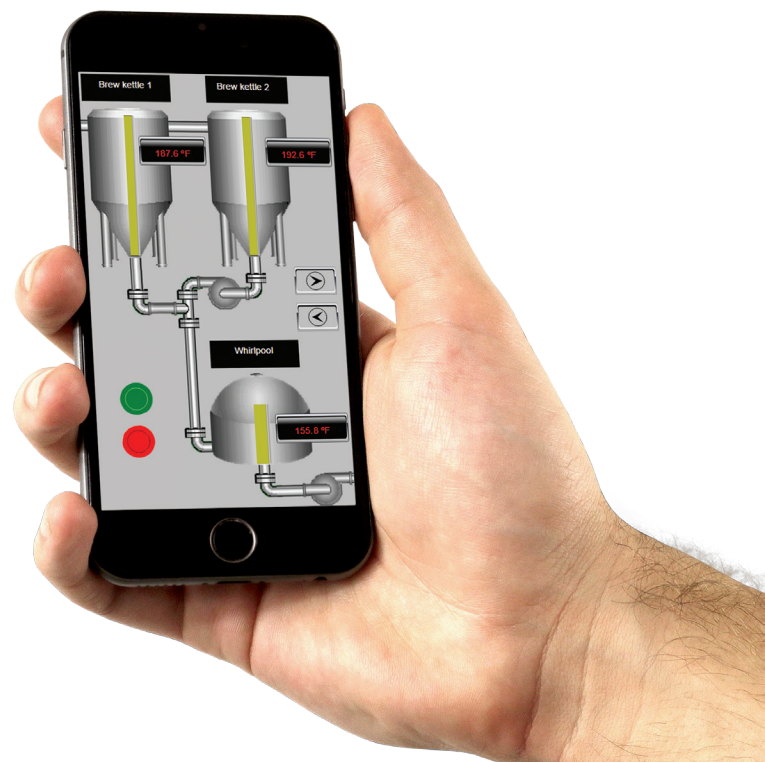
NOTABLE FEATURES

Regulations and standards have required many sectors, such as energy and water supply, to take concrete security measures.

We are building our Web OCS products to be a feature component of the connected industrial landscape. Secured network connections with user and access control are integral elements of Horner Web OCS, and we are including high standards of security that our customers will need.

Security Features

- Layer-based protection concept
- Ethernet load limitation
- Securing of network services by means of authentication and end-to-end encryption (SSL)
- Access control
- Protection functions at system level
- Open interfaces for access control and cryptographic functions in user applications
- Predefined security levels for basic protection

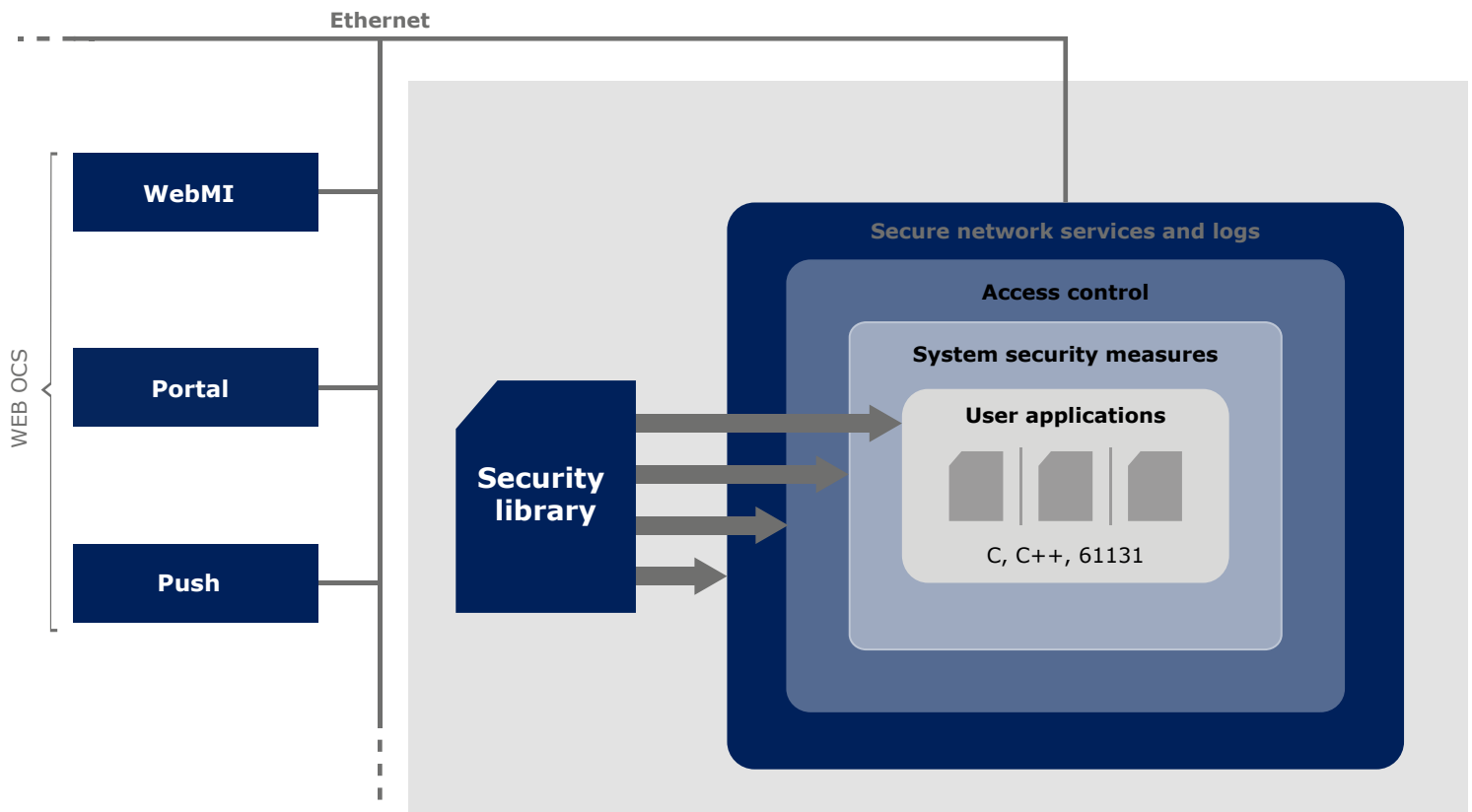


COMMUNICATION AND INFORMATION SECURITY

A targeted attack to a machine controller or an unintentional operating error can cause a production standstill or even destruction of a machine or plant, leading to a potential loss of reputation and money. With WebMI security the main objective is to ensure a robust system of protection. With preventative measures to protect data and communication, Horner helps make unauthorized access more difficult so your company quickly can spot and correct problems.

TARGETED ACCESS

Exposed machines and plants are not subject to the same perimeter protection as enclosed industrial plants. The greatest risk in production plants mainly comes from the inside. Service staff from an external service provider or a disgruntled employee may launch a targeted act of damage to property. The targets here are switches, routers and controllers with free ports. These can be used for inconspicuous disruption or for interception of communications.



HOW WEBMI WORKS

WebMI works by using the microSD card in the OCS as the web server. In other words, the web site files and graphics are hosted on the SD card in the controller.

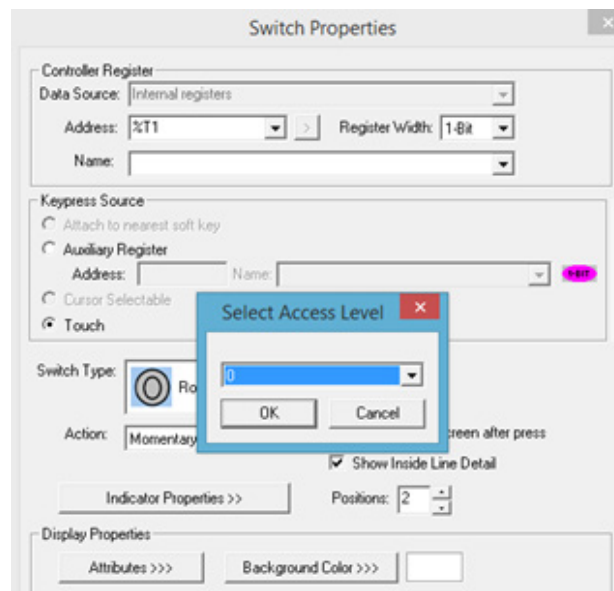
An OCS application is downloaded or copied directly to the microSD to the unit with FTP configured on the LAN port as standard. The application contains the controller logic and graphics. A second Cscape application is also be created for the Web site files and graphics. This is separate to the OCS program and the graphics need not be the same. However, for relating data and registers in the controller application to the objects on the web site, the registers must correspond. The Web page files are published directly from Cscape to the SD card in the OCS, using FTP.

The Web page files are published directly from Cscape to the SD card in the OCS, using FTP. Once the web page files have been successfully transferred to the SD card in the controller, the interface can be remotely viewed from any PC, or wireless device, connected to the same local network.

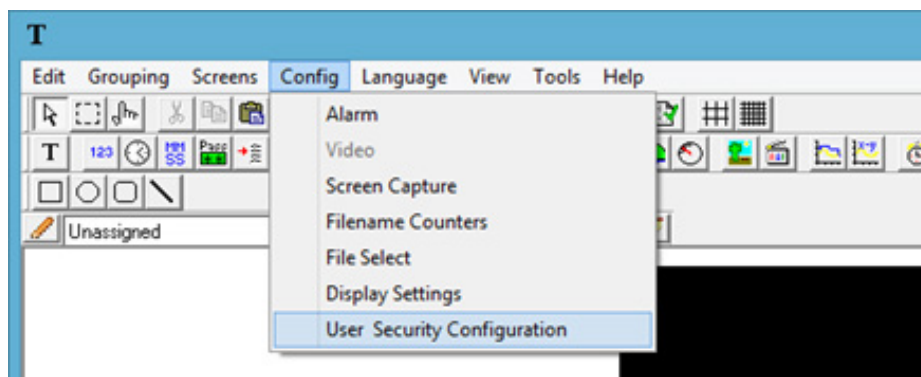
LEVEL-BASED ACCESS

Level-based access is one of the new functionalities to be available in the newest Cscape release. It allows a list of users to be created and configured with their associated passwords and access levels.

Graphics objects on the user screens can also be configured to have an associated access level. This level will determine which users can interact with this screen object, based on their own access level. For example, if a touch button is configured to have a user access level of 4, only OSC users that have logged in as a user with access level 4 or higher can select this button object.



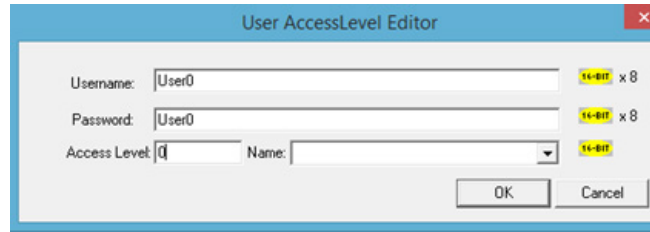
Assigning an Object's Access Level



Where to Configure Users and Access Levels

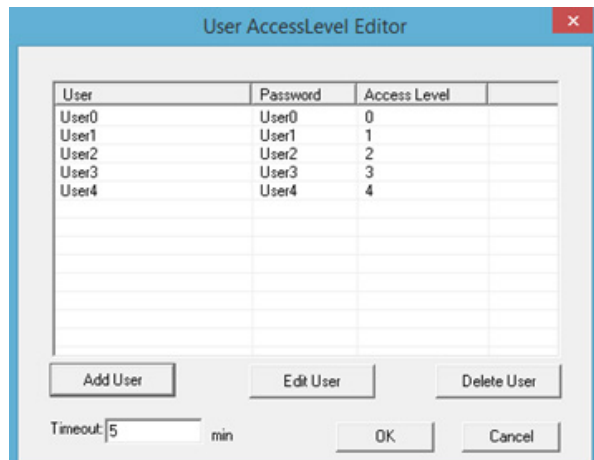
The table of users, their passwords and access levels are set up via the graphics editor. Select the 'Config' tab and choose 'User Security Configuration'.

This will open a blank configuration table. To configure a user, select the 'Add User' button and the following window will open. Create a username, password and assign an access level to the user. Here an access level of 0 was selected, which is the lowest level of access. Access level 0 is the default access level for all graphics objects unless configured as otherwise.



Username: User0 x8
 Password: User0 x8
 Access Level: 0 Name: x8
 OK Cancel

Adding a User



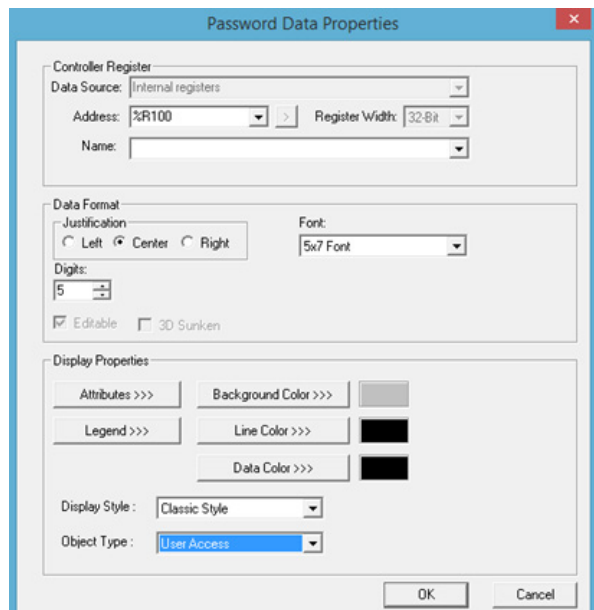
User	Password	Access Level
User0	User0	0
User1	User1	1
User2	User2	2
User3	User3	3
User4	User4	4

Add User Edit User Delete User
 Timeout: 5 min OK Cancel

Table of Configured Users

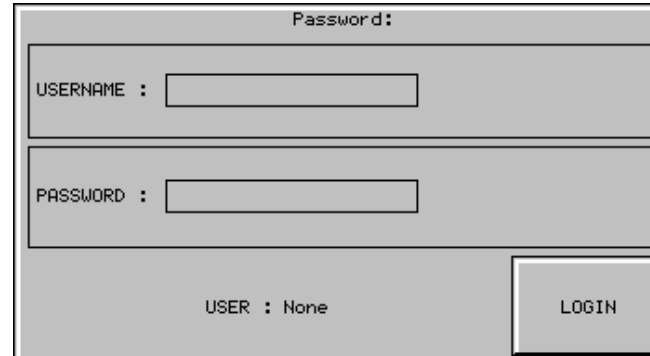
Up to 255 users can be configured and there are 8 different access levels, 0-7. The figure below shows the table of configured users, of which there are 5 here. There is also an option in this window to set the timeout for the login session. In the image below this timeout is set to 5 minutes which means that if a user is logged in and is inactive for 5 minutes or more, the OCS will automatically log the user out.

There is a dedicated screen object in order to allow the OCS user to login with a particular access level. This object contains fields for both the username and password and once a particular user has logged in, the object will also display the currently logged in user. This graphics object is shown in the figure below.



Controller Register
 Data Source: Internal registers
 Address: %R100 Register Width: 32-Bit
 Name:
 Data Format
 Justification: Left Center Right
 Font: 5x7 Font
 Digits: 5
 Editable 3D Sunken
 Display Properties
 Attributes >>> Background Color >>>
 Legend >>> Line Color >>>
 Data Color >>>
 Display Style: Classic Style
 Object Type: User Access
 OK Cancel

Password Data Properties



Username:
 Password:
 USER : None LOGIN

Level-based Access User Login Object

To create this object on a user screen, select the 'Password Data' object from the toolbar in the graphics editor. Once the object is placed on the user screen, double-click on the object to open the object's properties window. The following window will appear.

To configure the password object for user-access login, select 'User Access' from the 'Object Type' dropdown list, as shown in the figure above.

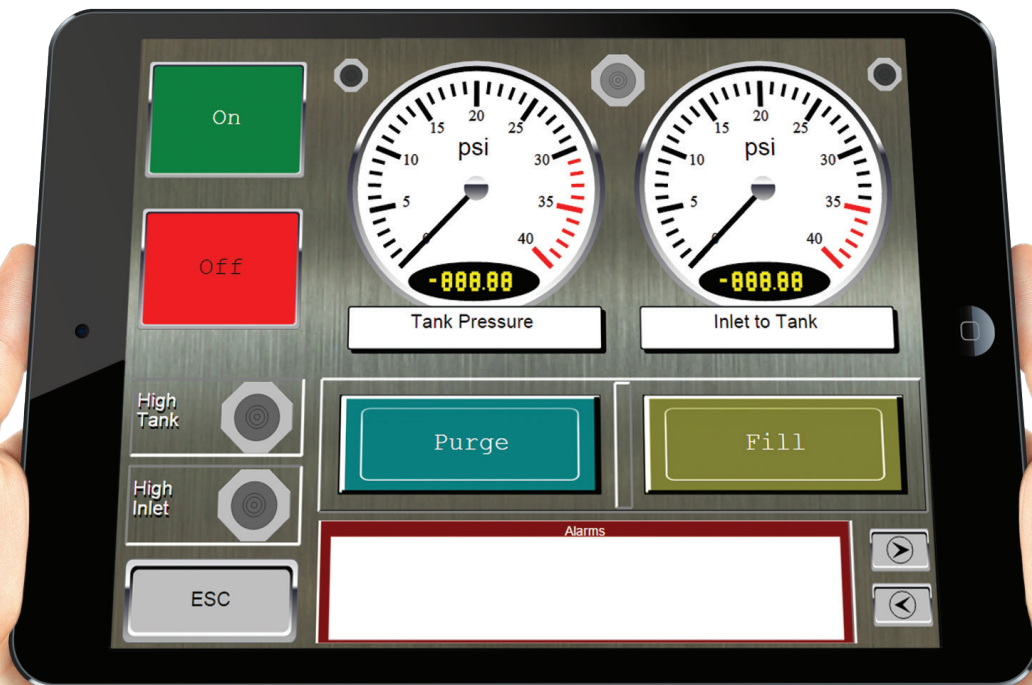
ENCRYPTION

WebMI passwords are stored on the microSD card and encrypted using a highly secure method, which turns normal text into a 32-digit hexadecimal number. Even if someone were to steal the microSD card from the unit, they wouldn't be able to see or retrieve any passwords with any practical level of ease. Horner is working constantly to stay on top of the latest security methodologies that are available.

The communication through the web browser to the OCS is encrypted through 128-bit Secure Sockets Layer (SSL) security, which means that each browser session is protected by a 128-bit key exchanged by the client and server with 2^{128} possible key combinations, which is 340,282,366,920,938,463,463,374,607,431,768,211,456 combinations. This is a secure method of encrypting web traffic used throughout the technology industry.

MOVING FORWARD

With the launch of WebMI, Horner continues its efforts in the Internet of Things. Enhanced security and innovative software designs coupled with Horner's industry leading OCS controllers have allowed our company to surpass others in the industry.



TERMS AND CONDITIONS OF USE POLICY

INTRODUCTION AND ACCEPTANCE

Unless otherwise agreed to in writing by the Horner APG ("HORNER APG"), by using the HORNER WEBMI, HORNER PUSH and Horner Portal of HORNER APG, you agree to the following Terms and Conditions of Use Policy without limitation or qualification. Please read these terms and conditions carefully before using HORNER APG's HORNER WEBMI, HORNER PUSH or Horner Portal. If you do not agree with the Terms and Conditions of Use Policy, you are not granted permission to use HORNER APG's HORNER WEBMI, HORNER PUSH and Horner Portal. All references in this Terms and Conditions of Use Policy to "we," "us," or "our" shall refer to HORNER APG and its subsidiaries. All references in this Terms and Conditions of Use Policy to "you" or "your" shall refer to the users of HORNER APG's HORNER WEBMI, HORNER PUSH and Horner Portal.

EXCLUSION OF WARRANTIES AND LIMITATIONS OF LIABILITY

HORNER APG's HORNER WEBMI, HORNER PUSH and Horner Portal are provided by HORNER APG on an "as is" and "as available" basis. HORNER APG makes no representations or warranties of any kind, express or implied, as to the operation of HORNER APG's HORNER WEBMI, HORNER PUSH or Horner Portal or the information, content, materials, or services included thereon, including, but not limited to, implied warranties of merchantability and fitness for a particular purpose. In particular, HORNER APG does not warrant that HORNER APG's HORNER WEBMI, HORNER PUSH or Horner Portal, its servers, or email sent from HORNER APG are free of viruses or other harmful components. HORNER APG will not be liable for any damages of any kind arising from the use of, or inability to use, HORNER APG's HORNER WEBMI, HORNER PUSH or Horner Portal, including, but not limited to, direct, indirect, incidental, punitive, and consequential damages, whether in contract, tort, or otherwise. Certain state laws do not allow limitations on implied warranties or the exclusion or limitation of certain damages; accordingly, the above limitations or exclusions may not apply to you.

GENERAL USE OF THE HORNER WEBMI, HORNER PUSH AND HORNER PORTAL

1. In order to access certain features of HORNER APG's HORNER WEBMI, HORNER PUSH and Horner Portal, you may be required to provide information about yourself (such as identification or contact details) as part of the registration process, including to obtain a HORNER APG account to access certain sections of the HORNER WEBMI, HORNER PUSH and Horner Portal, or as part of your continued use of such HORNER WEBMI, HORNER PUSH or Horner Portal. You agree that any registration information you give to HORNER APG will always be accurate, correct, and up to date.
2. You agree to use HORNER APG's HORNER WEBMI, HORNER PUSH and Horner Portal only for purposes that are permitted by (a) this Terms and Conditions of Use Policy, and (b) any applicable law, regulation, or generally accepted practices or guidelines in the relevant jurisdictions (including any laws regarding the export of data or software to and from the United States or other relevant countries).
3. You agree not to access (or attempt to access) HORNER APG's HORNER WEBMI, HORNER PUSH or Horner Portal by any means other than through the interface that is provided by HORNER APG. You specifically agree not to access (or attempt to access) any part of HORNER APG's HORNER WEBMI, HORNER PUSH or Horner Portal through any automated means (including use of scripts or web crawlers) and shall ensure that you comply with the instructions set out in any robots.txt file present on such HORNER WEBMI, HORNER PUSH or Horner Portal.
4. You agree that you will not engage in any activity that interferes with or disrupts HORNER APG's HORNER WEBMI, HORNER PUSH or Horner Portal (or the servers and networks which are connected to such HORNER WEBMI, HORNER PUSH or Horner Portal).
5. You agree that you will not reproduce, duplicate, copy, republish, upload, post, transmit, distribute, modify, sell, trade, or resell HORNER APG's HORNER WEBMI, HORNER PUSH or Horner Portal, or any portion, feature, or content thereof, for any purpose; provided that you may download one copy of the materials on HORNER APG's HORNER WEBMI, HORNER PUSH or Horner Portal on any single computer for your non-commercial use only and you may print one copy of the materials on HORNER APG's HORNER WEBMI, HORNER PUSH or Horner Portal for your non-commercial use only; further provided that you keep intact all copyright and other proprietary notices on any such downloaded or printed materials.
6. You agree that you are solely responsible for (and that HORNER APG has no responsibility to you or to any third-party for) any breach of your obligations under the Terms and Conditions of Use Policy and for the consequences (including any loss or damage which HORNER APG may suffer) of any such breach.
7. You must be 18 years or older and of legal consent age to use HORNER APG's HORNER WEBMI, HORNER PUSH or Horner Portal unsupervised. If you are under the age of 18, you may only use such HORNER WEBMI, HORNER PUSH and Horner Portal in conjunction with, and under the supervision of, your parents or guardians.
8. You must be a human. HORNER APG accounts registered by "bots" or other automated methods are not permitted.
9. Your HORNER APG account may only be used by one person - a single HORNER APG account shared by multiple people is not permitted.
10. You agree and understand that you are responsible for maintaining the confidentiality and security of your HORNER APG account and password, if any. HORNER APG cannot and will not be liable for any loss or damage from your failure to comply with this security obligation.
11. You agree that you will be solely responsible to HORNER APG for all activities that occur under your HORNER APG account.
12. If you become aware of any unauthorized use of your HORNER APG account or password, you agree to notify HORNER APG immediately.
13. We reserve the right to modify or discontinue, temporarily or permanently, your access to HORNER APG's HORNER WEBMI, HORNER PUSH or Horner Portal, or your HORNER APG account with or without notice.

COMMENTS, COMMUNICATIONS, AND OTHER CONTENT

Certain features within HORNER APG's HORNER WEBMI, HORNER PUSH or Horner Portal may allow you to post comments, send emails and other communications, and submit suggestions, ideas, comments, questions, or other information (together "Commenting"). You agree, understand and represent that all of your Commenting: (i) is accurate, (ii) is owned or otherwise controlled by you, (iii) is not illegal, obscene, threatening, defamatory, invasive of privacy, infringing of intellectual property rights, or otherwise injurious to third-parties, and (iv) does not consist of or contain software viruses, political campaigning, commercial solicitation, chain letters, mass mailings, or any form of "spam." You may not use a false e-mail address, impersonate any person or entity, or otherwise mislead as to the origin of Commenting. HORNER APG reserves the right (but not the obligation) to monitor and edit or remove any Commenting activity or content. If you do post Commenting content or submit Commenting material, you grant HORNER APG a nonexclusive, royalty-free, perpetual, irrevocable, and fully sublicensable right to use, reproduce, modify, adapt, publish, translate, create derivative works from, distribute, and display such Commenting content throughout the world in any media, including the right to use the name that you submit in connection with such Commenting. HORNER APG takes no responsibility and assumes no liability for any commenting content posted by you or any third-party.

LINKS

HORNER APG's HORNER WEBMI, HORNER PUSH and Horner Portal may be linked to other HORNER WEBMI, HORNER PUSHs not maintained by us. We do not control and are not responsible for the content of and policies governing use of those HORNER WEBMI, HORNER PUSHs not maintained by us. The inclusion of any link to such HORNER WEBMI, HORNER PUSHs does not imply approval of or endorsement by us of the HORNER WEBMI, HORNER PUSHs or the content thereof.

PRIVACY

Please read our Privacy Policy which also governs your use of HORNER APG's HORNER WEBMI, HORNER PUSH and Horner Portal to understand our policies about what information we collect, how we will treat this information, and what options you have to direct our activities.

OWNERSHIP, COPYRIGHT AND TRADEMARK

All content included on HORNER APG's HORNER WEBMI, HORNER PUSH and Horner Portal, such as trademarks, service marks, trade names, text, graphics, logos, icons, button icons, images, data compilations, domain names, and software, is the property of HORNER APG or its content suppliers or used with permission. The compilation of all content on this site is the exclusive property of HORNER APG and may be protected by U.S. and international copyright laws. All software used on this site is the property of HORNER APG or their software suppliers and may be protected by United States and international copyright laws. Nothing on this site should be construed as granting any license or right to such content or software.

COPYRIGHT AND TRADEMARK COMPLAINTS

The Horner APG respects the intellectual property of others. If you believe that your work has been copied in a way that constitutes copyright infringement on HORNER APG's HORNER WEBMI, HORNER PUSH or Horner Portal, please notify us immediately by phone at 877-665-5666 or by mail at Horner APG 59 South State Avenue Indianapolis, IN 46201

SITE TECHNOLOGIES

HORNER APG hereby disclaims any rights to trademarks, service marks, trade names, logos, copyrights, patents, domain names, or other intellectual property interests of third-parties.

APPLICABLE LAW

By using HORNER APG's HORNER WEBMI, HORNER PUSH or Horner Portal, you agree that the laws of the State of Indiana, without regard to principles of conflict of laws, will govern this Terms and Conditions of Use Policy and any dispute of any sort that might arise between you and HORNER APG regarding such Policy.

CHANGES TO THE TERMS

We reserve the right, at any time, to modify, alter, or update these Terms and Conditions of Use Policy without prior notice. Modifications shall become effective immediately upon being posted on our HORNER WEBMI, HORNER PUSH and Horner Portal. Your continued use of the HORNER WEBMI, HORNER PUSH and Horner Portal after modifications are posted constitutes an acknowledgement and acceptance of the Terms and Conditions of Use Policy and its modifications.

UPDATED

July 15, 2015

HOW TO CONTACT US

Any questions about this Terms and Conditions of Use Policy should be addressed to sales@heapg.com or by mail at: Horner APG, 59 South State Avenue Indianapolis, IN 46201