# Plant an App
# Security Specification

Revision: 29th of November, 2017

Our top priority for Plant an App is security. Without it, nothing else matters. We've spent quite a bit of time experimenting with various technologies and setups to achieve the highest level of security available today. This document describes all the security layers we've put in place.

## Shared Responsibility Model

Security and Compliance is a shared reponsibility between Amazon Web Services, Plant an App and the customer. The shared model relieves the customer the technical aspects of the security, such as managing web servers, running websites and web applications, physical server security, data redundancy, network security, operating system, deploying updates and so on.

The customer assumes responsibility for granting access to the system to authorized personel and revoking these permissions when need arises. We recommend the least access principle which states that users should gain access only to the resources they need to manage.

## Amazon Security

We've built our hosting infrastructure on top of Amazon Web Services which has the most advanced data centers and network architecture today. Security is the top priority. Network firewalls allow creating private networks that are isolated from the rest of the servers in the AWS cloud. Then there's strategies for DDos mitigation, data encryption, identity and access control, monitoring, logging and dozens of other services that are available out of the box and already integrated with the new servers that we maintain.

So, moving a website on AWS will usually boost security as it's usually very expensive to get the same level of security for on-premise or small hosting environments.

For further reading check the Amazon Web Services security page.

## DDoS Protection

We've taken a number of measures to prevent DDoS attacks in all layers of our infrastructure. These measures include:

- Disabled ICMP traffic to prevent ping attacks
- Using AWS Route 53 to prevent DNS attacks
- Using Cloudfront CDN to prevent DDoS on static files
- Using AWS Shield through load balancer in front of all public web applications, which helps protect against common DDoS attacks, such as SYN flood and UDP reflection attacks

## VPN

Except HTTP and HTTPS, we block all traffic that comes from the internet. To access other services such as Remote Desktop, FTP or SSMS, our clients are required to connect to the VPN using SSTP protocol, which is the safest tunneling technology available.

Even after the VPN connection is established, the only ports that are open are those for services we support. Additional ports can be opened on request.

## Virtual Machines

All our clients are hosted on dedicated Virtual Machines. This means there are no shared disk drives, memory or other resources that can be exploited. This kind of isolation eliminates the security and performance risks associated with shared hosting and allows for further security adjustments to be performed at VM level without affecting other clients.

The Virtual Machines run Windows Server 2016 that are kept up-to-date. The update window is agreed with each customer.

## Isolated Application Pools

A Virtual Machine can hold one or more websites. Each website is isolated, so it only has read/write access to its folder. This means that a vulnerability in a DNN instance can't propagate to other websites or to the operating system.

## SSL

HTTPS should be standard as it's the one of most effective forms of protection. Google also takes this into account when calculating rankings. We encourage all clients to use HTTPS. For standard plans we even include a 2048-bit SSL certificate to make sure all websites hosted with us have the highest level of security.

Our standard communications happen over TLS 1.2, though TLS 1.0 and 1.1 are still available on request in order to be able to communicate with legacy system from the outside world.

We also provide tools to enforce SSL and make browser cookies available only on HTTPS to prevent protocol downgrade attacks.

## Powerful Firewall

As we do our hosting on Amazon Web Services, we get the benefit of using built-in Security Groups which act as virtual firewalls. These firewalls are maintained by Amazon, so they don't take up server resources like Windows Firewall does. They filter unwanted traffic even before it reaches the network interface of the web servers.

## Security Updates

We deploy security updates ASAP for all clients that we host. This includes Windows, .NET, DNN and DNN Sharp modules. We do it free of charge because our top priority is security.

## Default Services

In this section we list the services that are provided by default on our servers. Each service has the associated ports open for internet and VPN traffic..

From the internet:

- HTTP and HTTPS
- VPN SSTP

From the VPN connection:

- SSMS for database access
- FTP for file transfer
- RDP for remote desktop access

Additional services and ports can be opened on request.

## Technology Stack

Our platform is built on Microsoft .NET technology stack which comes with enterprise level security features. Some of these features we inherited from the DNN layer and SQL Server, while others we used to secure DNN Sharp modules and the hosting infrastructure.

## Security at Application Level

DNN Sharp components feature various features that can be implemented to create new layers of security. These include:

- Two Factor Authentication (2FA) can be implemented using the forms and SMS gateway integration
- Blockchain API can be used to ensure data integrity at any snapshot in time
- Encryption actions that can be used in any workflow based component such as forms, data grids, APIs or scheduled tasks
- The Credential Store that can be used to securely store passwords or secret API keys.

# Compliance

Plant an App infrastructure it inherits the comprehensive cloud compliance structure put in place by Amazon Web Services.

Amazon Web Services Cloud Compliance enables customers to understand the robust controls in place at AWS to maintain security and data protection in the cloud. As systems are built on top of AWS cloud infrastructure, compliance responsibilities will be shared.

By tying together governance-focused, audit-friendly service features with applicable security compliance regulations or audit standards, AWS Compliance enablers build on traditional programs, helping customers to establish and operate in an AWS security control environment.

Following is a list of current assurance programs.

## Certifications / Attestations

- C5 [Germany]
- Cyber Essentials Plus [UK]
- DoD SRG
- FedRAMP
- FIPS
- IRAP [Australia]
- ISO 9001
- ISO 27001
- ISO 27017
- ISO 27018
- MTCS [Singapore]
- PCI DSS Level 1
- SEC Rule 17-a-4(f)
- SOC 1
- SOC 2
- SOC 3

## Laws, Regulations, and Privacy

- CISPE

- EU Model Clauses
- FERPA
- GLBA
- HIPAA
- HITECH
- IRS 1075
- ITAR
- My Number Act [Japan]
- U.K. DPA - 1988
- VPAT / Section 508
- EU Data Protection Directive
- Privacy Act [Australia]
- Privacy Act [New Zealand]
- PDPA - 2010 [Malaysia]
- PDPA - 2012 [Singapore]
- PIPEDA [Canada]
- Spanish DPA Authorization

## Alignments / Frameworks

- CIS
- CJIS
- CSA
- ENS [Spain]
- EU-US Privacy Shield
- FFIEC
- FISC
- FISMA
- G-Cloud [UK]
- GxP (FDA CFR 21 Part 11)
- ICREA
- IT Grundschutz [Germany]
- MITA 3.0
- MPAA
- NIST
- PHR
- Uptime Institute Tiers
- UK Cloud Security Principles

For more information about compliance, please read AWS Cloud Compliance.