```
### SILVERSTRIPE START ###
# Deny access to templates (but allow from localhost)
<Files *.ss>
  Order deny,allow
  Deny from all
  Allow from 127.0.0.1
</Files>

# Deny access to IIS configuration
<Files web.config>
  Order deny,allow
  Deny from all
</Files>

# Deny access to YAML configuration files which might include sensitive information
<Files *.yml>
  Order allow,deny
  Deny from all
</Files>

# Route errors to static pages automatically generated by SilverStripe
ErrorDocument 404 /assets/error-404.html
ErrorDocument 500 /assets/error-500.html

<IfModule mod_rewrite.c>
  SetEnv HTTP_MOD_REWRITE On
  RewriteEngine On
  RewriteBase '/'



  # Deny access to potentially sensitive files and folders
  RewriteRule ^vendor(/|$) - [F,L,NC]
  RewriteRule silverstripe-cache(/|$) - [F,L,NC]
  RewriteRule composer\.(json|lock) - [F,L,NC]

  # Process through SilverStripe if no file with the requested name exists.
  # Pass through the original path as a query parameter, and retain the existing
parameters.
  RewriteCond %{REQUEST_URI} ^(.*)$
  RewriteCond %{REQUEST_FILENAME} !-f
```

```
  RewriteCond %{REQUEST_FILENAME} !-f
  RewriteRule .* framework/main.php?url=%1 [QSA]
</IfModule>
### SILVERSTRIPE END ###
```