

MICROS Systems, Inc. Product Versioning Convention & PA-DSS Validation Policy

**Products: MICROS Point-Of-Sale Products Which Process Credit Cards:
(i.e.) RES, e7, 9700, Symphony**

Versioning Convention:

Version: A.B.CCDD.EEEE

A = Major Release

B = Feature Release

CC = Maintenance Release

DD = Beta Release or Hot Fix Number

EEEE = Development Build Number

Product Release Publication:

Major Releases: Approximately 1 Every 1-2 Years

Feature Releases: Approximately 3-4 Every Year

Maintenance Releases: Approximately 8-9 Per Year

Hot Fixes: Approximately 1-2 Every Week

Product Release Descriptions:

Major Releases: Major releases will contain significant new capabilities, such as major new features and functionality, additional operating system or database support, additional product modules, significant work flow or user interface improvements, etc. Defect corrections will be included.

Feature Releases: Feature releases will contain new capabilities and enhancements, such as additional features and functionality, etc. Defect corrections will be included.

Maintenance Releases: Maintenance releases will only contain defect corrections to existing features and functionality.

Hot Fixes: A Hot fix is a small software change which corrects a single issue or defect. Hot fixes are not general released and are provided on a case-by-case basis.



Policy Regarding Software Changes Impacting Security Or Cardholder Data:

- Software changes which impact either security or cardholder data will only be generally released as part of a Major Release, or a Feature Release, both of which will not be generally released until achieving validation under the Payment Card Industry Payment Application Data Security Standard, (PCI PA-DSS).

Policy Regarding PCI PA-DSS Validations:

MICROS has elected not to validate all of its released products under the Payment Card Industry Payment Application Data Security Standard, (PCI PA-DSS). This is due to the length of time it takes to have these products tested and validated. MICROS cannot adequately service its customers with tactical enhancements and fixes, while having all of these tactical releases validated. Therefore, MICROS has adopted the policy shown below:

- All Major Releases will be PCI PA-DSS validated prior to general release.
- All Feature Releases will be PCI PA-DSS validated prior to general release.
- Maintenance Releases will not be PCI PA-DSS validated.
- Beta Releases and Hot Fixes will not be PCI PA-DSS validated.
- Development builds are not in scope of the PCI PA-DSS and are not validated.

Policy Regarding PCI PA-DSS Re-Validations:

- Products validated against the PCI PA-DSS must be re-validated each year, in order to remain acceptable for new deployments. For each general release product that MICROS has validated against the PCI PA-DSS, MICROS will endeavor to re-validate these products at least two more times. Therefore, these products should be PCI PA-DSS validated for a minimum period of three years from the date of initial PCI PA-DSS validation. We believe this time-based, as opposed to version-based policy is much better for our customers.

Note: MICROS may deem, (at its sole discretion), not to re-validate a previously validated product if changes are made to the PCI PA-DSS requirements that make continued re-validation of that particular MICROS product unfeasible.



Policy Regarding Installations:

- Only a PA-DSS validated product should be installed for new installations whenever feasible. This is intended to prevent Acquirers/Processors from potentially refusing to board a new merchant.

Policy Regarding Listing of PABP or PA-DSS Validated MICROS Products:

- The Payment Card Industry Security Standards Council, (PCI SSC), now charges a substantial recurring fee to payment application vendors to list their validated products on the PCI SSC web site. MICROS had originally chosen not to list its PCI PA-DSS validated products on the PCI SSC web site. Instead, MICROS had listed all Visa PABP and PCI PA-DSS validated products on its web site at the following link:

<http://www.micros.com/ServicesAndSupport/InformationSecurity/PABPPADSSCertifiedProducts/>

MICROS is continuing to list its validated products on its own web site. However, MICROS has reached an agreement with the PCI-SSC regarding listing terms and fees and effective April 2009, MICROS is now listing its PA-DSS validated applications on the PCI-SSC web site at the following link:

https://www.pcisecuritystandards.org/security_standards/vpa/



Products: Property Management System Products Which Process Credit Cards: (i.e.) Opera

Versioning Convention:

Version A.B.C.DD.EXX.2102009

A = Major Release

B = Development Release (no longer used)

C = Revision rollup (rollup of 4 previous service packs)

D = Service pack (contains both new features and defect corrections)

E10 = E-patch, also referred to as a hot fix

2102009 = Development build (numbered as per the date)

Product Release Publication:

Major Releases: Approximately 1 every 2 years

Revision Rollup: Approximately 1 every year

Service Packs: Approximately 3-4 per year

E-Patches: Approximately 1 every week

Product Release Descriptions:

Major Releases: Major releases will contain significant new capabilities, such as major new features and functionality, new operating system or database support, additional product modules, as well as defect corrections, etc.

Revision Rollups: Revision rollups will contain a rollup of the previous 4 Service Packs.

Service Packs: Service pack revisions will contain both new capabilities and enhancements, (including additional features and functionality), as well as defect corrections.

E-Patches: E-Patches will contain corrections for critical defects, as well as certain smaller enhancements, (that do not impact either security or cardholder data), that may be needed immediately by the customer.



Policy Regarding Software Changes Impacting Security Or Cardholder Data:

- Software changes which impact either security or cardholder data will only be generally released as part of a Major Release, or a Service Pack, both of which will not be generally released until achieving validation under the Payment Card Industry Payment Application Data Security Standard, (PCI PA-DSS).

Policy Regarding PCI PA-DSS Validations:

MICROS has elected not to validate all of its released products under the Payment Card Industry Payment Application Data Security Standard, (PCI PA-DSS). This is due to the length of time it takes to have these products tested and validated. MICROS cannot adequately service its customers with tactical enhancements and fixes, while having all of these tactical releases validated. Therefore, MICROS has adopted the policy shown below:

- Major Releases will be PCI PA-DSS validated prior to general release.
- Development Releases will not be PCI PA-DSS validated.
- Revision Rollups will be PCI PA-DSS validated prior to general release.
- Service Packs will be PCI PA-DSS validated prior to general release.
- E-Patches will not be PCI PA-DSS validated.
- Development builds are not in scope of the PCI PA-DSS and are not validated.

Policy Regarding PCI PA-DSS Re-Validations:

- Products validated against the PCI PA-DSS must be re-validated each year, in order to remain acceptable for new deployments. For each general release product that MICROS has validated against the PCI PA-DSS, MICROS will endeavor to re-validate these products at least 2 more times. Therefore, these products should be PCI PA-DSS validated for a minimum period of 3 years from the date of initial PCI PA-DSS validation. We believe this time-based, as opposed to version-based policy is much better for our customers.

Note: MICROS may deem, (at its sole discretion), not to re-validate a previously validated product if changes are made to the PCI PA-DSS requirements that make continued re-validation of that particular MICROS product unfeasible.



Policy Regarding Installations:

- Only a PA-DSS validated product should be installed for new installations whenever feasible. This is intended to prevent Acquirers/Processors from potentially refusing to board a new merchant.

Policy Regarding Listing of PABP or PA-DSS Validated MICROS Products:

- The Payment Card Industry Security Standards Council, (PCI SSC), now charges a substantial recurring fee to payment application vendors to list their validated products on the PCI SSC web site. MICROS had originally chosen not to list its PCI PA-DSS validated products on the PCI SSC web site. Instead, MICROS had listed all Visa PABP and PCI PA-DSS validated products on its web site at the following link:

<http://www.micros.com/ServicesAndSupport/InformationSecurity/PABPPADSSCertifiedProducts/>

MICROS is continuing to list its validated products on its own web site. However, MICROS has reached an agreement with the PCI-SSC regarding listing terms and fees and effective April 2009, MICROS is now listing its PA-DSS validated applications on the PCI-SSC web site at the following link:

https://www.pcisecuritystandards.org/security_standards/vpa/