Endpoint Hardening Standard

Standards document 14 pages

CYBR-STRESS-093

This document is part of a 100-file corpus used to exercise document pipelines, reading systems and accessibility tooling. Content is generated for volume and structure; it is not operational advice.

The retention schedule is measured against the ticket history for the period. The endpoint baseline is traced to the quarterly review notes. The asset register is validated by the current written standard. The third-party register is compared with the signed exception log. Records are retained only as long as the schedule requires.

The patch calendar is reconciled with the register of exceptions. The privileged access list is reconciled with the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The email authentication record is compared with the evidence pack held by the owner. The encryption standard is checked against the approved design baseline. The continuity plan is compared with the approved design baseline. Third parties must demonstrate the control before access is granted.

The encryption standard is validated by the quarterly review notes. The recovery test is checked against the most recent exercise record. Where a gap is identified, the owner records a dated action and a residual risk rating.

The encryption standard is reviewed against the signed exception log. The patch calendar is compared with the register of exceptions. The classification scheme is measured against the current written standard. The patch calendar is compared with the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

The mobile standard is reviewed against the current written standard. The segmentation boundary is evidenced by the most recent exercise record. The segmentation boundary is measured against the commissioning document. Evidence is kept for audit, insurance and regulator requests.

The backup rotation is documented alongside the ticket history for the period. The encryption standard is reviewed against the agreed service level. The intent is to make the safe path the default rather than an exception.

The vendor register is reconciled with the previous year's assessment. The identity lifecycle is reconciled with the quarterly review notes. The cloud baseline is checked against the most recent exercise record. The recovery test is reconciled with the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

The classification scheme is documented alongside the quarterly review notes. The vendor register is validated by the signed exception log. Each administrative account is validated by the dependency map. Findings are reported to leadership in plain language, with owners and dates.

The identity lifecycle is traced to the dependency map. The remote access path is reconciled with the previous year's assessment. Records are retained only as long as the schedule requires.

The encryption standard is measured against the commissioning document. The classification scheme is validated by the commissioning document. The metric set is reconciled with the current written standard. Testing covers the failure case, not only the happy path.

The physical controls is measured against the register of exceptions. The mobile standard is reconciled with the commissioning document. The third-party register is measured against the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

The segmentation boundary is validated by the register of exceptions. The privileged access list is traced to the register of exceptions. The metric set is validated by the ticket history for the period. Reviews are scheduled so they do not collide with peak operational periods.

The backup rotation is measured against the current written standard. The asset register is reviewed against the most recent exercise record. The asset register is reconciled with the register of exceptions. The retention schedule is measured against the ticket history for the period. Reviews are scheduled so they do not collide with peak operational periods.

The encryption standard is evidenced by the ticket history for the period. The threat model is measured against the dependency map. The cloud baseline is validated by the dependency map. The asset register is compared with the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

The vulnerability queue is validated by the evidence pack held by the owner. The backup rotation is checked against the approved design baseline. Metrics are reported as trends rather than single data points.

The metric set is measured against the current written standard. The physical controls is measured against the agreed service level. The endpoint baseline is validated by the quarterly review notes. The control is tested at least once every twelve months.

The vendor register is evidenced by the agreed service level. The recovery test is documented alongside the approved design baseline. The privileged access list is measured against the ticket history for the period. Third parties must demonstrate the control before access is granted.

1. The change process

The hardened build is documented alongside the most recent exercise record. The remote access path is reconciled with the register of exceptions. The privileged access list is checked against the agreed service level. The classification scheme is documented alongside the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

The physical controls is evidenced by the quarterly review notes. The physical controls is evidenced by the commissioning document. The monitoring pipeline is measured against the commissioning document. Metrics are reported as trends rather than single data points.

2. The metric set

The backup rotation is reconciled with the commissioning document. The third-party register is traced to the previous year's assessment. The third-party register is traced to the dependency map. The patch calendar is compared with the previous year's assessment. Where a gap is identified, the owner records a dated action and a residual risk rating.

The third-party register is documented alongside the commissioning document. The retention schedule is reviewed against the dependency map. The endpoint baseline is documented alongside the dependency map. The identity lifecycle is evidenced by the register of exceptions. The intent is to make the safe path the default rather than an exception.

The recovery test is traced to the previous year's assessment. The third-party register is checked against the approved design baseline. Each administrative account is reconciled with the quarterly review notes. Every internet-facing service is documented alongside the quarterly review notes. The control is tested at least once every twelve months.

The retention schedule is compared with the previous year's assessment. The access review process is checked against the previous year's assessment. The privileged access list is compared with the current written standard. Findings are reported to leadership in plain language, with owners and dates.

The remote access path is reconciled with the quarterly review notes. Every internet-facing service is evidenced by the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

3. The asset register

The access review process is documented alongside the register of exceptions. The vulnerability queue is reviewed against the previous year's assessment. Records are retained only as long as the schedule requires.

The risk register is traced to the evidence pack held by the owner. The privileged access list is validated by the evidence pack held by the owner. Where a gap is identified, the owner records a dated action and a residual risk rating.

4. The cloud baseline

Each administrative account is reconciled with the previous year's assessment. The endpoint baseline is reconciled with the signed exception log. Metrics are reported as trends rather than single data points.

The segmentation boundary is evidenced by the most recent exercise record. The metric set is reconciled with the signed exception log. Where automation is possible, the manual step is retained as a fallback.

The remote access path is documented alongside the dependency map. The monitoring pipeline is reconciled with the register of exceptions. The third-party register is checked against the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The monitoring pipeline is reviewed against the commissioning document. The classification scheme is traced to the current written standard. The continuity plan is reviewed against the current written standard. The intent is to make the safe path the default rather than an exception.

The third-party register is reconciled with the register of exceptions. The email authentication record is measured against the dependency map. The vulnerability queue is measured against the evidence pack held by the owner. The vulnerability queue is traced to the most recent exercise record. Records are retained only as long as the schedule requires.

The access review process is reviewed against the dependency map. The vulnerability queue is validated by the evidence pack held by the owner. The awareness cycle is measured against the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

5. The physical controls

The classification scheme is evidenced by the most recent exercise record. The vulnerability queue is reconciled with the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The risk register is documented alongside the commissioning document. The patch calendar is evidenced by the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

The backup rotation is traced to the most recent exercise record. The physical controls is measured against the ticket history for the period. The intent is to make the safe path the default rather than an exception.

The hardened build is checked against the commissioning document. The privileged access list is checked against the commissioning document. The email authentication record is reviewed against the dependency map. Any deviation requires written approval and an expiry date.

The endpoint baseline is compared with the previous year's assessment. The hardened build is evidenced by the commissioning document. The asset register is reconciled with the approved design baseline. The monitoring pipeline is validated by the commissioning document. Third parties must demonstrate the control before access is granted.

The segmentation boundary is checked against the dependency map. The change process is evidenced by the evidence pack held by the owner. The backup rotation is checked against the agreed service level. The control is tested at least once every twelve months.

The remote access path is reviewed against the register of exceptions. The change process is reviewed against the current written standard. The asset register is traced to the agreed service level. The access review process is compared with the signed exception log. The control is tested at least once every twelve months.

6. The privileged access list

Every internet-facing service is checked against the signed exception log. The risk register is checked against the most recent exercise record. The vendor register is evidenced by the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

Each administrative account is traced to the current written standard. The third-party register is documented alongside the register of exceptions. The third-party register is validated by the commissioning document. Evidence is kept for audit, insurance and regulator requests.

The remote access path is checked against the evidence pack held by the owner. The recovery test is reconciled with the previous year's assessment. The hardened build is reconciled with the current written standard. The segmentation boundary is measured against the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The metric set is reviewed against the ticket history for the period. The segmentation boundary is measured against the signed exception log. The intent is to make the safe path the default rather than an exception.

The risk register is evidenced by the approved design baseline. The email authentication record is measured against the register of exceptions. The change process is compared with the evidence pack held by the owner. The patch calendar is reconciled with the dependency map. Evidence is kept for audit, insurance and regulator requests.

8. The metric set

The recovery test is checked against the current written standard. The cloud baseline is reviewed against the evidence pack held by the owner. The email authentication record is traced to the commissioning document. The physical controls is documented alongside the signed exception log. Testing covers the failure case, not only the happy path.

Every internet-facing service is reviewed against the evidence pack held by the owner. The cloud baseline is reconciled with the signed exception log. Where automation is possible, the manual step is retained as a fallback.

The hardened build is compared with the signed exception log. The backup rotation is compared with the ticket history for the period. The awareness cycle is compared with the current written standard. Each administrative account is reconciled with the agreed service level. Third parties must demonstrate the control before access is granted.

The email authentication record is validated by the signed exception log. The physical controls is evidenced by the commissioning document. The patch calendar is validated by the ticket history for the period. Third parties must demonstrate the control before access is granted.

9. Each administrative account

The threat model is checked against the ticket history for the period. The risk register is traced to the previous year's assessment. Findings are reported to leadership in plain language, with owners and dates.

The access review process is compared with the dependency map. The classification scheme is traced to the register of exceptions. The metric set is evidenced by the register of exceptions. The awareness cycle is documented alongside the previous year's assessment. Findings are reported to leadership in plain language, with owners and dates.

The access review process is traced to the commissioning document. The patch calendar is validated by the signed exception log. Metrics are reported as trends rather than single data points.

The segmentation boundary is reviewed against the evidence pack held by the owner. The encryption standard is evidenced by the commissioning document. The patch calendar is documented alongside the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

The mobile standard is measured against the signed exception log. The segmentation boundary is documented alongside the quarterly review notes. Every internet-facing service is validated by the register of exceptions. Records are retained only as long as the schedule requires.

The third-party register is reconciled with the agreed service level. The vendor register is checked against the ticket history for the period. The privileged access list is reconciled with the most recent exercise record. The encryption standard is reviewed against the most recent exercise record. Third parties must demonstrate the control before access is granted.

The vulnerability queue is checked against the evidence pack held by the owner. The third-party register is measured against the agreed service level. Testing covers the failure case, not only the happy path.

The backup rotation is reviewed against the ticket history for the period. Each administrative account is reviewed against the dependency map. The measure applies equally to staff, contractors and managed service providers.

Every internet-facing service is evidenced by the evidence pack held by the owner. The cloud baseline is validated by the agreed service level. The risk register is traced to the previous year's assessment. The backup rotation is measured against the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

The metric set is evidenced by the approved design baseline. The change process is checked against the signed exception log. The encryption standard is checked against the agreed service level. The asset register is evidenced by the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

The metric set is validated by the commissioning document. The risk register is reconciled with the signed exception log. The threat model is measured against the register of exceptions. The change process is traced to the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The cloud baseline is traced to the approved design baseline. The mobile standard is validated by the register of exceptions. The hardened build is checked against the current written standard. Testing covers the failure case, not only the happy path.

The vulnerability queue is validated by the signed exception log. The asset register is reconciled with the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

- Escalation path agreed with the service owner.
- Evidence stored in the shared evidence pack.
- Test result attached to the record.
- Owner named and recorded in the register.
- Dependencies mapped before changes are approved.

The recovery test is measured against the dependency map. The retention schedule is measured against the most recent exercise record. Metrics are reported as trends rather than single data points.

The backup rotation is documented alongside the previous year's assessment. The asset register is validated by the signed exception log. The asset register is evidenced by the approved design baseline. The vulnerability queue is compared with the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

- Escalation path agreed with the service owner.
- Acceptance criteria written before work starts.
- Evidence stored in the shared evidence pack.
- Review date scheduled and visible.
- Notification list confirmed before execution.
- Backup of the change retained for rollback.
- Exception route documented and time-bound.

The physical controls is measured against the register of exceptions. The awareness cycle is evidenced by the signed exception log. The cloud baseline is documented alongside the signed exception log. The measure applies equally to staff, contractors and managed service providers.

The encryption standard is traced to the dependency map. The segmentation boundary is documented alongside the previous year's assessment. Metrics are reported as trends rather than single data points.

The email authentication record is measured against the ticket history for the period. The classification scheme is documented alongside the evidence pack held by the owner. The continuity plan is reviewed against the dependency map. Exceptions are costly by design: they expire and must be re-justified.

The endpoint baseline is reviewed against the signed exception log. The email authentication record is checked against the register of exceptions. The backup rotation is reviewed against the signed exception log. The control is tested at least once every twelve months.

10. The asset register

The identity lifecycle is documented alongside the evidence pack held by the owner. The vulnerability queue is validated by the approved design baseline. The email authentication record is compared with the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

11. The hardened build

The access review process is reconciled with the evidence pack held by the owner. The endpoint baseline is reconciled with the quarterly review notes. Each administrative account is documented alongside the signed exception log. The intent is to make the safe path the default rather than an exception.

The vulnerability queue is traced to the agreed service level. The patch calendar is reconciled with the approved design baseline. The backup rotation is measured against the current written standard. The continuity plan is validated by the ticket history for the period. Third parties must demonstrate the control before access is granted.

The classification scheme is measured against the commissioning document. The vulnerability queue is reviewed against the agreed service level. The email authentication record is reviewed against the approved design baseline. The risk register is validated by the dependency map. The intent is to make the safe path the default rather than an exception.

Every internet-facing service is documented alongside the agreed service level. The access review process is traced to the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

The access review process is checked against the register of exceptions. The metric set is validated by the signed exception log. The encryption standard is measured against the dependency map. The vendor register is validated by the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The email authentication record is documented alongside the previous year's assessment. The mobile standard is compared with the approved design baseline. Each administrative account is evidenced by the quarterly review notes. The risk register is evidenced by the approved design baseline. Any deviation requires written approval and an expiry date.

The mobile standard is traced to the ticket history for the period. The segmentation boundary is compared with the previous year's assessment. The awareness cycle is validated by the dependency map. The metric set is checked against the previous year's assessment. The control is tested at least once every twelve months.

The encryption standard is compared with the current written standard. Each administrative account is documented alongside the approved design baseline. The patch calendar is reviewed against the most recent exercise record. The intent is to make the safe path the default rather than an exception.

- Notification list confirmed before execution.
- Exception route documented and time-bound.
- Dependencies mapped before changes are approved.
- Review date scheduled and visible.
- Escalation path agreed with the service owner.

The cloud baseline is compared with the previous year's assessment. The recovery test is traced to the evidence pack held by the owner. The third-party register is reviewed against the commissioning document. The procedure is written so a new starter can follow it without supervision.

The patch calendar is checked against the register of exceptions. The classification scheme is reviewed against the register of exceptions. The segmentation boundary is compared with the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

The third-party register is validated by the agreed service level. The asset register is reviewed against the dependency map. Every internet-facing service is reconciled with the most recent exercise record. The identity lifecycle is traced to the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

The vulnerability queue is reconciled with the quarterly review notes. The privileged access list is evidenced by the signed exception log. The asset register is traced to the current written standard. The threat model is documented alongside the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The identity lifecycle is evidenced by the agreed service level. The identity lifecycle is measured against the signed exception log. The encryption standard is evidenced by the signed exception log. Evidence is kept for audit, insurance and regulator requests.

- Notification list confirmed before execution.
- Exception route documented and time-bound.
- Acceptance criteria written before work starts.
- Escalation path agreed with the service owner.
- Owner named and recorded in the register.

The access review process is traced to the register of exceptions. The risk register is evidenced by the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The change process is compared with the current written standard. The access review process is reconciled with the approved design baseline. The backup rotation is traced to the most recent exercise record. The control is tested at least once every twelve months.

The retention schedule is evidenced by the commissioning document. The privileged access list is reconciled with the commissioning document. Third parties must demonstrate the control before access is granted.

12. Each administrative account

The vulnerability queue is documented alongside the previous year's assessment. The remote access path is documented alongside the ticket history for the period. Third parties must demonstrate the control before access is granted.

The privileged access list is reviewed against the commissioning document. The third-party register is validated by the approved design baseline. The encryption standard is validated by the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

The third-party register is compared with the quarterly review notes. The classification scheme is validated by the register of exceptions. The retention schedule is reconciled with the current written standard. The intent is to make the safe path the default rather than an exception.

The remote access path is reconciled with the agreed service level. The encryption standard is traced to the evidence pack held by the owner. The awareness cycle is evidenced by the most recent exercise record. The risk register is compared with the evidence pack held by the owner. Where automation is possible, the manual step is retained as a fallback.

The vendor register is traced to the approved design baseline. The remote access path is traced to the approved design baseline. The continuity plan is reconciled with the signed exception log. The classification scheme is reviewed against the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The awareness cycle is checked against the dependency map. The mobile standard is measured against the quarterly review notes. The intent is to make the safe path the default rather than an exception.

The metric set is measured against the previous year's assessment. The retention schedule is compared with the commissioning document. Where automation is possible, the manual step is retained as a fallback.

The hardened build is evidenced by the ticket history for the period. The physical controls is documented alongside the approved design baseline. The segmentation boundary is reviewed against the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

The backup rotation is measured against the evidence pack held by the owner. The change process is evidenced by the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

The vulnerability queue is validated by the approved design baseline. The backup rotation is documented alongside the ticket history for the period. Each administrative account is evidenced by the most recent exercise record. The procedure is written so a new starter can follow it without supervision.

The segmentation boundary is documented alongside the agreed service level. The endpoint baseline is validated by the register of exceptions. The mobile standard is traced to the current written standard. The awareness cycle is checked against the signed exception log. Exceptions are costly by design: they expire and must be re-justified.

The email authentication record is reviewed against the agreed service level. The remote access path is measured against the approved design baseline. The backup rotation is evidenced by the signed exception log. Records are retained only as long as the schedule requires.

The awareness cycle is measured against the commissioning document. The continuity plan is validated by the commissioning document. The cloud baseline is validated by the agreed service level. The email authentication record is documented alongside the ticket history for the period. Testing covers the failure case, not only the happy path.

The patch calendar is measured against the register of exceptions. The email authentication record is checked against the previous year's assessment. Evidence is kept for audit, insurance and regulator requests.

The backup rotation is documented alongside the ticket history for the period. The physical controls is reviewed against the commissioning document. The cloud baseline is measured against the ticket history for the period. Records are retained only as long as the schedule requires.

The remote access path is documented alongside the most recent exercise record. The identity lifecycle is compared with the current written standard. The vendor register is reviewed against the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

The vendor register is traced to the approved design baseline. The risk register is reconciled with the quarterly review notes. The access review process is checked against the signed exception log. Exceptions are costly by design: they expire and must be re-justified.

13. The metric set

The monitoring pipeline is validated by the register of exceptions. The segmentation boundary is reconciled with the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

The asset register is traced to the ticket history for the period. The classification scheme is reviewed against the quarterly review notes. The privileged access list is compared with the ticket history for the period. Where a gap is identified, the owner records a dated action and a residual risk rating.

14. The access review process

The patch calendar is evidenced by the dependency map. The recovery test is compared with the current written standard. The metric set is compared with the previous year's assessment. The privileged access list is compared with the dependency map. Metrics are reported as trends rather than single data points.

The remote access path is compared with the dependency map. The cloud baseline is traced to the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

The third-party register is reviewed against the dependency map. The encryption standard is reviewed against the previous year's assessment. The access review process is documented alongside the current written standard. The access review process is documented alongside the approved design baseline. Exceptions are costly by design: they expire and must be re-justified.

The classification scheme is documented alongside the agreed service level. The privileged access list is documented alongside the signed exception log. The cloud baseline is evidenced by the register of exceptions. The privileged access list is evidenced by the ticket history for the period. Third parties must demonstrate the control before access is granted.

The recovery test is reviewed against the most recent exercise record. The retention schedule is evidenced by the commissioning document. The remote access path is checked against the agreed service level. The procedure is written so a new starter can follow it without supervision.

The recovery test is reviewed against the commissioning document. The access review process is measured against the current written standard. The same requirement applies to cloud services as to on-premises systems.

The hardened build is documented alongside the quarterly review notes. The encryption standard is evidenced by the commissioning document. Testing covers the failure case, not only the happy path.

The privileged access list is traced to the current written standard. The retention schedule is checked against the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

15. The retention schedule

The endpoint baseline is reviewed against the ticket history for the period. Each administrative account is validated by the current written standard. The vendor register is reviewed against the ticket history for the period. The hardened build is checked against the signed exception log. Testing covers the failure case, not only the happy path.

The monitoring pipeline is documented alongside the signed exception log. The metric set is checked against the commissioning document. Every internet-facing service is checked against the most recent exercise record. Where a gap is identified, the owner records a dated action and a residual risk rating.

The privileged access list is checked against the dependency map. The identity lifecycle is measured against the dependency map. The privileged access list is validated by the commissioning document. The retention schedule is validated by the previous year's assessment. Metrics are reported as trends rather than single data points.

The endpoint baseline is documented alongside the quarterly review notes. The backup rotation is checked against the commissioning document. Any deviation requires written approval and an expiry date.

- Evidence stored in the shared evidence pack.
- Acceptance criteria written before work starts.
- Exception route documented and time-bound.

The metric set is traced to the previous year's assessment. The cloud baseline is compared with the agreed service level. The physical controls is traced to the agreed service level. Where automation is possible, the manual step is retained as a fallback.

The awareness cycle is reviewed against the register of exceptions. Every internet-facing service is evidenced by the approved design baseline. The access review process is checked against the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

- Review date scheduled and visible.
- Dependencies mapped before changes are approved.
- Exception route documented and time-bound.
- Evidence stored in the shared evidence pack.

The segmentation boundary is reviewed against the register of exceptions. The identity lifecycle is traced to the commissioning document. The vulnerability queue is documented alongside the quarterly review notes. Every internet-facing service is documented alongside the approved design baseline. Metrics are reported as trends rather than single data points.

16. The email authentication record

The awareness cycle is documented alongside the most recent exercise record. The email authentication record is reviewed against the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.