Architectuurprincipes VISTA college

Hierbij is Architectuur een consistent geheel van uitgangspunten (principes) en modellen dat richting geeft aan ontwerp en realisatie van de processen, organisatorische inrichting, informatievoorziening en technische infrastructuur van een organisatie.

VISTA college volgt de referentie architectuur MORA en hanteert de volgende Architectuur principes:

1. VISTA college digitaliseert haar diensten en processen
2. VISTA college gaat op een vertrouwelijke manier met gegevens om.
   Waaronder, broneigenaarschap is benoemd en geborgd voor wat betreft de persoonsgegevens van studenten en medewerkers
3. VISTA college gebruikt generieke processen en functies.
4. VISTA college hergebruikt gegevens.
5. VISTA college voert regie over uitbestede diensten.
6. VISTA college informatievoorziening is geïntegreerd.

   VISTA college informatie is geïntegreerd beschikbaar in een gepersonaliseerd portaal;
   Applicaties zijn geïntegreerd met andere applicaties die voor de gebruiker relevante gegevens of functionaliteit bevatten;
   Applicaties halen gegevens uit de authentieke bron met de vanuit het proces gewenste actualiteit;
   Applicaties bieden gestandaardiseerde koppelvlakken (services) op basis van open of de facto standaarden;
   Applicaties die zelf geen gestandaardiseerde koppelvlakken bieden worden geïntegreerd middels integratievoorzieningen en conform een goed gedefinieerd gegevensmodel (wanneer beschikbaar middels een Enterprise Service Bus VISTA college, SURFeduhub, Open Onderwijs API);
   Applicaties ondersteunen het proces of maken gebruik van een Business Process Management systeem;
   Alleen de functionaliteit die in een bepaalde processtap noodzakelijk is wordt aangeboden vanuit een applicatie.

7. De informatievoorziening overschrijdt organisatiegrenzen, zoals toekomstige (landelijke) ontwikkelingen: eduID en centraal aanmelden studenten.
8. VISTA college gebruikers hebben toegang tot de informatievoorziening.
   Mensen willen steeds meer leren en werken op het tijdstip en de plaats waarop het hen het beste uitkomt (any time, any place, any device). Het moge duidelijk zijn dat dit alleen toegang en gebruik is tot die onderdelen op basis van hun functie en rol.
9. VISTA college gegevens zijn beveiligd op basis van hun risicoclassificatie.
10. Applicaties voor onderwijs en bedrijfsvoering zijn gestandaardiseerd.
11. ICT voorzieningen zijn marktconform.
12. Primaire bedrijfsprocessen worden niet verstoord door de implementatie van veranderingen.

    Primaire bedrijfsprocessen zijn de kern van de organisatie en verstoringen hierin hebben een grote impact op de organisatie. Organisaties veranderen continu en frequente verstoringen zijn onacceptabel. Nieuwe processen en systemen worden niet geïmplementeerd tenzij ze zijn getest en goedgekeurd. Onbeschikbaarheid van applicaties wordt geminimaliseerd gedurende installatie of vervanging, en wordt bij voorkeur buiten kantooruren uitgevoerd.

13. Er wordt een VISTA college enterprise portaal gefaciliteerd.
14. Expliciete bewaking van service niveaus.

    Alle gebeurtenissen die relevant zijn voor het bewaken van de serviceniveaus worden expliciet bewaakt. Daarnaast moet in het algemeen de beschikbaarheid, capaciteit en performance worden bewaakt en moet het mogelijk zijn om de oorzaak van verstoringen te kunnen analyseren. Hiertoe is

het belangrijk dat applicaties de juiste informatie loggen om analyses uit te kunnen voeren. Zonder deze logging is de detectie en diagnose van problemen zeer tijdrovend of zelfs onmogelijk.

15. Geïntegreerde gebruikerservaring inclusief selfservice voorziening
16. Het enterprise portaal ontsluit alleen generieke veelgebruikte functionaliteit.
17. Applicaties zijn weggebaseerd.
18. Bron bepaald toegang.
    De autorisaties van de bronapplicatie zijn leidend. De integriteit en vertrouwelijkheid van informatie moet worden bewaakt.
19. Gegevens hebben een eigenaar.
20. Gegevens worden voorzien van een rubricering
    De beschikbaarheid, integriteit en vertrouwelijkheid van gegevens moet worden geborgd. Rubricering van gegevens behelst het toekennen van een standaard risicoclassificatie aan informatie.
21. Gegevens worden onderhouden in de bron applicaties
22. Webbased applicaties tenzij
    Slechts in uitzonderlijke situaties worden client/ server oplossingen geboden
23. Binnen de informatievoorziening (IV) en het ICT landschap VISTA college wordt het beleid cloud tenzij gehanteerd.
24. Microsoft tenzij, waaronder vastgestelde standaard operating system voor Microsoft servers, standaard Microsoft database en Microsoft 365. Ten opzichte van de recente software versie (V) wordt ondersteund de eerst voorgaande en de eerst volgende versie. Hierbij wordt de levenscyclus van de fabrikant gevolgd (waarbij standaard support is afgedekt).

25. Er wordt gebruik genaakt van een digitaal fundament VISTA college, dit zijn de basis en generieke ICT voorzieningen. **Zie punt 37 toelichting digitaal fundament VISTA college**

    Eventuele benodigde virtuele servers (IaaS) worden afgenomen via Surfcumulus.

26. Afgenomen VISTA college diensten worden minimaal één keer per jaar geaudit door het VISTA college zelf dan wel door een externe audit partij.
27. Voor alle afgenomen As A Service varianten geldt de eis dat deze fysiek zijn ondergebracht in de Europese Economische Ruimte (EER).
28. Meerdere beveiligingsstrategieën. Beveiliging dient niet afhankelijk te zijn van enkelvoudige maatregelen omdat compromitteren dan tot totale onveiligheid leidt. Beveiliging die niet end-to-end is kan worden gecompromitteerd in de tussenliggende lagen.
29. Filtering tussen zones, Er zijn expliciete netwerkzones gedefinieerd, inclusief regels die aangeven welke IT componenten in een bepaalde zone mogen staan en welk soort communicatie tussen netwerkzones is toegestaan. Op de grens tussen zones staat netwerkapparatuur die in staat is om netwerkverkeer te filteren dat niet voldoet aan de regels.
30. Informatiebeveiliging en privacy beleid VISTA college is ingeregeld en geborgd. Het VISTA college volgt tevens de richtlijnen vanuit het NCSC waaronder de ICT-beveiligingsrichtlijnen voor webapplicaties (NCSC, 2019). Door compartimentering toe te passen, wordt voorkomen dat het compromitteren van een server, applicatie of toepassing in één compartiment, directe gevolgen heeft voor servers, webapplicaties en toepassingen in een ander compartiment.
31. Rol gebaseerde autorisatie. Het hebben van een identiteit is niet voldoende om toegang te krijgen tot een systeem; er is ook een autorisatie noodzakelijk. Door autorisaties te baseren op de rol van de gebruiker hoeven autorisaties niet op individueel niveau te worden toegekend, waardoor autorisatiebeheer efficiënter kan plaats vinden. Hierdoor is de organisatie ook beter in staat om de rechtmatigheid van uitgegeven autorisaties te controleren. Toegang en gebruik is gebaseerd op organisatorische eenheid, functie en rol.
32. Bij aanschaf van nieuwe applicaties en/of afnemen van diensten wordt gelet op een aantal eigenschappen: toekomstvastheid; (open) standaarden; bewezen technologie; marktconform;

marktaandeel; betrouwbaarheid leverancier; de aansluiting op het bestaande applicatie- en diensten landschap; selfservice componenten voor eindgebruikers en exit strategie.

33. Bij applicatie- c.q. dienstenontwikkeling is tijdig een functioneel en technisch ontwerp beschikbaar. Iedere ontwikkeling is vooraf vertaald in een functioneel en technisch ontwerp passend binnen de doel architectuur. Het VISTA college ontwikkelt niet zelf.
34. Changemanagement, ontwikkelingen en wijzigingen worden vooraf gepland, goedgekeurd, doorgevoerd, getest en al dan niet geaccepteerd middels een changeprocedure. Bij een wijziging wordt een impact en risico analyse uitgevoerd. SCOPAFIJTH model (Security, Communicatie, Organisatie, Personeel, Administratieve organisatie, Financiën, Informatievoorziening, Juridisch, Technologie en Huisvesting.
35. Processen hebben een proceseigenaar. Ieder proces kent een proces eigenaarschap groep.
36. Systeemeigenaarschap. Binnen het VISTA college is systeemeigenaarschap belegd. De systeemeigenaar is verantwoordelijk voor: beschikbaarheid, beveiliging, naleving, onderhoud, backup/restore, up to date zijn van de omgeving en ondersteuning.

37. **Toelichting digitaal fundament VISTA college**

Het digitaal fundament VISTA college bevat

Basis ICT voorzieningen
bevat o.a. : AD, ADFS, AD connect, Azure AD, DNS/DHCP, Radius, Identity en Access Management (IAM), Surfcumulus (IaaS), Surfnet Internet en lichtpaden, VISTA werkplekken op VISTA locaties, VISTA werkplekken vanaf thuis, verbonden o.b.v. Always on VPN, Microsoft SCCM en SCOM, netwerk toegangscontrole, VPN, Quality of Service (QoS). *VISTA college voornemen, o.a. het implementeren van een "berichtenmakelaar", document management systeem en een datawarehouse.*

Generieke ICT voorzieningen
bevat o.a. : Microsoft 365 omgeving, Cloud print, scan en kopieer voorzieningen, Telefonie, Cardsonline, Topdesk, Mobile Device Management (Intune, KNOX, Schoolmaster), Antivirus, Federatie SURF/Surfconext en Kennisnet Entree, Site to Site VPN en Next Generation Firewall.

Aanvullende SaaS dienstverlening maakt gebruik van en wordt ingebed binnen het digitale fundament VISTA college

a) De (SaaS) applicatie laag bevindt zich in een ander compartiment dan de data laag (zie tevens h).
b) De (SaaS) applicatie maakt gebruik van onderliggende services uit het digitaal fundament VISTA college, bijvoorbeeld een beveiligde verbinding, centrale administratie identiteiten, andere SaaS functionaliteit.
c) Toegang en gebruik tot specifieke benodigdheden is specifiek ingeregeld (t.b.v. systeem of gebruikersgroep(en), inclusief eventuele afnemende systemen).
d) Specifieke benodigdheden t.b.v. het onderwijs zijn (logisch) gescheiden van de bedrijfsvoering.
e) Vanuit het digitaal fundament worden benodigde functionaliteiten gecentraliseerd (en geconsolideerd) ter beschikking gesteld aan de bovenliggende voorzieningen.
f) Legacy systemen hebben een houdbaarheidsdatum, aangezien we naar één IV/ICT landschap gaan waaronder plaats, tijd en device onafhankelijk werken. Hier worden nadere afspraken over gemaakt.
g) Voldoende overzicht en inzicht houden in het aantal actieve en niet meer actieve computer- en serversystemen dan wel via een (SaaS) dienst afgenomen ICT dienstverlening.
h) Compartimentering toepassen. Door compartimentering toe te passen, wordt voorkomen dat het compromitteren van een server, applicatie of functionaliteit in één compartiment, directe gevolgen heeft voor servers, webapplicaties en functionaliteit in een ander compartiment.
i) Online en offline back-ups.
j) Verbinding tussen Cloud oplossing (opdrachtnemer) t/m het centraal ICT knooppunt VISTA college is versleuteld en adequaat beveiligd (SURF, Surfcumulus).

k) Quality of Service op de eventuele Site 2 Site VPN verbinding (zie j) tussen Cloud (opdrachtnemer) t/m het centraal ICT knooppunt VISTA college.
l) Redundante Site to Site VPN verbinding aanwezig via een alternatieve route (zie j en k).
m) Firewall, DDoS mitigation, IDS, IPS, routering functionaliteit maakt onderdeel uit van de Cloud oplossing (opdrachtnemer), inzichtelijk voor Open Line (Advantive) en het VISTA college
n) Hardening van beveiligingscomponenten binnen de Cloud oplossing (opdrachtnemer). Hardening zorgt ervoor dat functionaliteiten die niet strikt noodzakelijk zijn niet meer aanwezig zijn, waardoor onnodige beveiligingsrisico's worden vermeden.
o) SCOM agent en SNMP (van kritische processen/services) functionaliteit wordt toegestaan binnen de Cloud oplossing (opdrachtnemer) zodat deze opgenomen wordt in de monitoring van Open Line (Advantive) lees VISTA college.
p) Cloud provider (opdrachtnemer) geeft de (technische) randvoorwaarden aan v.w.b. het type verbinding en de benodigde bandbreedte en configuraties bij piekbelasting tussen Cloud oplossing (opdrachtnemer) t/m het centraal ICT knooppunt VISTA college. VISTA college heeft theoretisch 14000 studenten en 1800 medewerkers. De eventuele Site 2 Site VPN verbinding vereist derhalve een adequate inrichting en werking (bedrijfszekerheid, conform SLA en DAP).
q) Verfijning van de windows domein rechten structuur (waaronder onderscheid in domein beheer- , onderhoud en gebruiker accounts). Accounts met beheer rechten maken standaard gebruik van twee factor authenticatie, dit geldt ook voor de Cloud omgeving (opdrachtnemer), Open Line (Advantive) en eventuele andere onderaannemers.
r) Bij een geïntegreerde informatievoorziening overzicht en inzicht in eventueel (gelijktijdige) activiteiten door meerdere partijen (m.b.t. relevante objecten, attributen, processen en services die door de betreffende Cloud provider worden geraakt). Er dient een proactief proces ingeregeld te zijn met de betrokken partijen, mochten bovengenoemde activiteiten elkaar “kruisen” en/of samenvallen en een bepaalde volgordelijkheid is vereist dan wel onderlinge afstemming tussen de relevante (externe) partijen.

Rolverdeling binnen het VISTA college en de relatie met relevante externe (ICT) partners

Het VISTA college is een regie organisatie, anno 2020 wordt deze verder doorontwikkeld.

Het organigram van het VISTA college is te achterhalen op de volgende website
https://vistacollege.nl/organisatorische-informatie/organogram

Binnen dit organigram is er de stafafdeling

Informatie Management en Management Informatie (IMMI), met de taken

- Focus op de toekomstige informatievoorziening
- Opstellen strategie en beleid op het terrein van de informatievoorziening
- Planvorming voor de realisatie van de gewenste situatie
- Ontwikkelen en verbeteren van bedrijfsprocessen (Business Proces (Re)Design)
- Fungeren als opdrachtgever namens de gebruikersorganisatie voor de uitvoerende teams ICT Functioneel Beheer (FB) en ICT Technisch Beheer (TB)
- Strategisch/Tactische aansturing van Leveranciers

Verder ligt in de lijn het ICT team

ICT Functioneel Beheer, met de taken

- Gericht op het beheer van organisatie eenheid overstijgende bedrijfsapplicaties systemen
- Beheer en optimalisatie van de bestaande informatievoorziening
- Realisatie/aansturen van wijzigingen in de inrichting van de eenheid overstijgende bedrijfsapplicaties
- Ontwikkelen en beheren van de werkprocessen
- Ondersteuning en scholing van de gebruikers

- Tactisch/operationele aansturing van leveranciers

ICT Technisch Beheer, met de taken

- Beheer en optimalisatie van de technische basisvoorzieningen incl. de bijbehorende management software.
- Zorgdragen voor optimale aansluiting van de technische voorzieningen op de wensen en behoeften van de organisatie.
- Aansturen/leiden van wijzigingen in de inrichting van de technische basisvoorzieningen.
- Ondersteuning en scholing van de gebruikers
- Tactisch/operationele aansturing van leveranciers

Bestaande afspraken tussen VISTA college en de externe ICT (kennis) partner Open Line (Advantive)

Vanuit beheer perspectief zijn er bestaande afspraken gemaakt met de huidige externe ICT (kennis) partner Open Line (onderaannemer Advantive). Conform de aanbesteding managed ICT infrastructuur diensten is namens VISTA college, Open Line ketenverantwoordelijk voor de ICT dienstverlening. Hierbij vervult Open Line de SIAM rol (Service Integration And Management), regie /coördinatie richting de (relevante) leveranciers/partners.

Stafdienst IMMI, Henry Jennen 2-6-2020